Fall 2010

Transfer Theory and its Applications to the Study of Simple Groups

Nicolas D. Meyer
Southern Illinois University Carbondale, ndmeyer1888@comcast.net

TRANSFER THEORY AND ITS APPLICATIONS TO THE STUDY OF SIMPLE GROUPS

by

Nicolas Meyer

B.S., Benedictine University, 2009

A Research Paper
Submitted in Partial Fulfillment of the Requirements for the
Master of Science Degree

Department of Mathematics
in the Graduate School
Southern Illinois University Carbondale
December, 2010

RESEARCH PAPER APPROVAL

TRANSFER THEORY AND ITS APPLICATIONS TO THE STUDY OF SIMPLE GROUPS

By

Nicolas Meyer

A Research Paper Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Master of Science

in the field of Mathematics

Approved by:

Dr. Robert Fitzgerald, Chair

Dr. John McSorley

Dr. Joseph Hundley

Graduate School
Southern Illinois University Carbondale
October 5, 2010

AN ABSTRACT OF THE RESEARCH PAPER OF

NICOLAS MEYER, for the Master of Science degree in MATHEMATICS, presented on OCTOBER 5TH, 2010, at Southern Illinois University Carbondale.

TITLE: TRANSFER THEORY AND ITS APPLICATIONS TO THE STUDY OF SIMPLE GROUPS

MAJOR PROFESSOR: Dr. R. Fitzgerald

This paper presents transfer theory and examines how it can be applied to the classification of simple groups.

ACKNOWLEDGMENTS

I would like to thank Dr. Fitzgerald for his invaluable assistance and insights leading to the writing of this paper. My sincere thanks also goes to Dr. McSorley and Dr. Hundley for their guidance as well as their patience in serving on my committee. I would also like to extend my gratitude to all the wonderful people in the Department of Mathematics. A special thanks goes to my family for their continued love and support.

TABLE OF CONTENTS

INTRODUCTION

The primary goal of this paper is to apply transfer theory to the study of simple groups. More specifically, we may use the results of transfer theory to determine whether or not certain numbers occur as orders of simple groups. Of course Sylow's Theorems are very useful in such determinations. We may aim to discover if transfer theory can provide more information in certain cases. One technique used to determine whether or not a group is simple is to search for a homomorphism having a proper, nontrivial kernel. Transfer theory is based on this idea and provides tools for establishing when the commutator subgroup is proper.

Chapter 1 will provide all the definitons and results that will be necessary in presenting transfer theory.

In Chapter 2 we will give a summary of transfer theory as it is given in *Algebra: A Graduate Course* by Martin Isaacs. Several examples will appear that will help illustrate the theory.

In Chapter 3 we will make many calculations to investigate how useful transfer theory can be in making certain claims about simplicity. More specifically, a complete analysis of the existence of simple groups for every possible order (from 1 to 200) will be given. An examination of certain orders beyond 200 will also be given. For those orders in which simple groups do not exist, the method of proof will be given. The aim is to see whether or not these proofs can be simplified with the use

of transfer theory. We may also like to know whether or not transfer theory is necessary in such proofs.

CHAPTER 1

BACKGROUND

Definition. Let G be a group and let p be a prime.

1. A group of order p^α for some $\alpha \geq 0$ is called a *p-group*. Subgroups of G which are p-groups are called *p-subgroups*.

2. If G is a group of order $p^\alpha m$ where p does not divide m, then a subgroup of order p^α is called a *Sylow p-subgroup of G*.

3. The set of Sylow p-subgroups of G will be denoted by $\mathrm{Syl}_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$.

Theorem 1.1. *(Sylow's Theorem)*

Let G be a group of order $p^\alpha m$, where p is a prime not dividing m.

1. *Sylow p-subgroups of G exist, i.e. $Syl_p(G) \neq \emptyset$.*

2. *If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.*

3. *The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e., $n_p(G) \equiv 1 \pmod p$. Further, $n_p(G)$ is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence $n_p(G)$ divides m.*

Corollary 1.2. *Let P be a Sylow p-subgroup of G. Then the following are equivalent:*

1. *P is the unique Sylow p-subgroup of G, i.e., $n_p(G) = 1$*
2. *P is normal in G*
3. *P is characteristic in G*
4. *All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.*

Definition. A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $(|G : H|, |H|) = 1$. (See [2])

Theorem 1.3. *Let $H < P$, where P is a finite p-group. Then $N_P(H) > H$.*

Definition. Let G be a group. We define the *commutator* of $x, y \in G$ to be $[x, y] = x^{-1}y^{-1}xy$. The subgroup generated by all the commutators of G is called the *commutator subgroup* or the *derived subgroup* of G and is denoted by G' or $[G, G]$.

Remark. It can be shown that the derived subgroup is the unique smallest normal subgroup of G such that the corresponding factor group is abelian.

Definition. A group G is *solvable* if ther exists a finite collection of normal subgroups $G_0, G_1, \ldots, G_n$ such that

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

and G_{i+1}/G_i is abelian for $0 \leq i < n$.

Remark. It is clear that abelian groups are solvable.

A group G is *nilpotent* if there exists a finite collection of normal subgroups $G_0, G_1, \ldots, G_n$, with

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

and such that

$$G_{i+1}/G_i \subseteq Z(G/G_i)$$

for $0 \leq i < n$.

Remark. It is easy to see that abelian groups are nilpotent and that nilpotent groups are solvable.

Theorem 1.4. *A finite p-group is nilpotent*

Definition. Set $Z_0(G) = 1$ and inductively define $Z_i(G)$ by the equation $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$ for $i > 0$. The collection $\{Z_i(G) \mid i \geq 0\}$ is called the *ascending* or *upper* central series of G.

Definition. Let $G^1 = G$, $G^2 = [G, G]$, $G^3 = [G^2, G]$, and in general, $G^i = [G^{i-1}, G]$ for $i > 1$. We have $G = G^1 \supseteq G^2 \supseteq G^3 \supseteq \cdots$. The *lower* or *descending* central series of G is the set of subgroups G^i.

Theorem 1.5. *Let G be any group and suppose $n \geq 1$. Then the following are equivalent:*

1. $G^{n+1} = 1$.

2. $Z_n(G) = G$.

Furthermore, G is nilpotent if and only if 1 and 2 hold for some integer n.

[1]

Theorem 1.6. *A finite group G is solvable if and only if for every divisor n of $|G|$ such that $(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n. (or a Hall subgroup)*

[2]

The group D_n will be useful in illustrating the theory with examples. We will let D_n denote the *dihedral group* of order $2n$. D_n is sometimes referred to as the group of symmetries of a reguar n-gon with $n \geq 3$. D_n is generated by two elements. We will denote the generators by r (a rotation of order n) and f (a flip of order 2). The following gives the group presentation of the dihedral group of order $2n$:

$$D_n = \langle r, f \mid r^n = f^2 = 1, rf = fr^{-1} \rangle$$

CHAPTER 2

TRANSFER THEORY

Most of the following material is an adaptation of [1].

Definition. If $H \subseteq G$, then a *right transversal T for H in G* is a set of right coset representatives for H in G.

Now, G acts on the set of right cosets of H in G by right multiplication. If T is a right transversal for H in G, then this action gives a right action of G on T. For $t \in T$ and $g \in G$, we define $t \cdot g$ to be the unique element of T that lies in the right coset Htg.

Lemma 2.1. *Let $H \subseteq G$ and suppose that T is a right transversal. If $t \in T$ and $x, y \in G$, then*

1. $t \cdot 1 = t$,
2. $(t \cdot x) \cdot y = t \cdot (xy)$, *and*
3. $tx(t \cdot x)^{-1} \in H$.

Proof. Statements 1 and 2 clearly hold since right multiplication by group elements on right cosets gives a group action. $t \cdot x \in Htx$, and so 3 now follows immediately. □

Suppose H is a subgroup of G of finite index. $tg(t \cdot g)^{-1} \in H$ for each $t \in T$ and $g \in G$. So we can define a map $\pi : G \to H$ by

$$\pi(g) = \prod_{t \in T} tg(t \cdot g)^{-1}.$$

Note that in the definition of π, we have not specified any particular order in which to carry out the multiplication. This will not be problematic since our intentions are to compose π with the canonical homomorphism from H into H/M where $M \lhd H$ with H/M abelian.

Definition. Let $H \subseteq G$ have finite index and suppose $M \lhd H$ with H/M abelian. The *transfer* from G to H/M is the map $v : G \to H/M$ given by $v(g) = M\pi(g)$, where

$$\pi(g) = \prod_{t \in T} tg(t \cdot g)^{-1}$$

and T is a right transversal for H in G.

Example 2.2. Consider the group $G = D_3$ generated by the rotation r and the flip f.

(a) Let $H = \langle r \rangle$, $M = 1$. We will compute the transfer from D_3 into $H/M = \langle r \rangle$. $T = \{1, f\}$ gives a transversal for $\langle r \rangle$ in D_3. In this case the transfer $v : D_3 \to \langle r \rangle$ is defined for $g \in D_3$ by $v(g) = \pi(g) = \prod_{t \in T} tg(t \cdot g)^{-1}$. We have $v(1) = (1 \cdot 1)^{-1}(f(f \cdot 1)^{-1}) = ff^{-1} = 1$. We have $v(r) = (r(1 \cdot r)^{-1})(fr(f \cdot r)^{-1}) = (r(1)^{-1})(frf^{-1}) = (r)(frf) = fr^{-1}rf = f^2 = 1$. So $v(r) = 1$. We see that $v(r^2) = ((r^2)(1 \cdot r^2)^{-1})((fr^2)(f \cdot r^2)^{-1}) = (r^2)(fr^2(f \cdot r^2)^{-1}) = r^2fr^2f^{-1} = r(rf)r^2f = r(fr^{-1})r^2f = rfrf = fr^{-1}rf = f^2 = 1$. So $v(r^2) = 1$. Similarly, $v(f) = (f(1 \cdot f)^{-1})(f^2(f \cdot f)^{-1}) = (ff^{-1})(f^2) = 1$. Also, $v(fr) = (fr(1 \cdot fr)^{-1})(ffr(f \cdot$

$fr)^{-1}) = fr(f^{-1})(ffr) = frfr = 1$. $v(fr^2) = (fr^2(1 \cdot fr^2)^{-1})(ffr^2(f \cdot fr^2)^{-1}) = (fr^2f)(r^2) = 1$. Hence, we see that the transfer map in this case is trivial.

(b) Now we will compute the transfer map in the case where $G = D_3$, $H = \langle f \rangle$, and $M = 1$. $T = \{1, r, r^2\}$ gives a right transversal for $\langle f \rangle$ in D_3. Again, the transfer $v : D_3 \to \langle f \rangle$ is defined for $g \in D_3$ by $v(g) = \pi(g) = \prod_{t \in T} tg(t \cdot g)^{-1}$. We have $v(1) = (1 \cdot 1)^{-1}(r(r \cdot 1)^{-1})(r^2(r^2 \cdot 1)^{-1}) = rr^{-1}r^2(r^2)^{-1} = 1$. We have $v(r) = (r(1 \cdot r)^{-1})(r^2(r \cdot r)^{-1})(r^3(r^2 \cdot r)^{-1})) = (rr^{-1})(r^2(r^2)^{-1}) = 1$. Thus, $v(r) = 1$. Likewise, $v(r^2) = (r^2(1 \cdot r^2)^{-1})(r^3(r \cdot r^2)^{-1})(r^4(r^2 \cdot r^2)^{-1}) = (r^2(r^2)^{-1})(r(r^{-1})) = 1$. Hence, $v(r^2) = 1$. We have $v(f) = (f(1 \cdot f)^{-1})(rf(r \cdot f)^{-1})(r^2f(r^2 \cdot f)^{-1}) = (f)(rf(r^2)^{-1})(r^2f(r^{-1})) = frf^2r^{-1} = f$. Therefore, $v(f) = f$. We see that $v(fr) = (fr(1 \cdot fr)^{-1})(rfr(r \cdot fr)^{-1})(r^2fr(r^2 \cdot fr)^{-1}) = (frr^{-1})(rfr)(r^2fr(r^2)^{-1}) = frfr^3fr^2 = fr^3 = f$. So $v(fr) = f$. Finally, $v(fr^2) = (fr^2(1 \cdot fr^2)^{-1})(rfr^2(r \cdot fr^2)^{-1})(r^2fr^2(r^2 \cdot fr^2)^{-1}) = (fr^3)(rfr^2(r^2))(r^2fr^2) = frfr^3fr^2 = frf^2r^2 = f$. Thus, $v(fr^2) = f$. So we see that the transfer map in this case is non-trivial. The transfer map is often times trivial, and we seek conditions to ensure that it is not.

Now we give the somewhat suprising result that the transfer is independent of the choice of transversal. It will be convenient to write $x \equiv y \bmod M$ if $x, y \in H$ with $Mx = My$.

Theorem 2.3. *Let S and T be right transversals for H in G and let $M \lhd H$ with H/M abelian. Assume $|G : H| < \infty$. Then for $g \in G$, we have $\prod_{t \in T} tg(t \cdot g)^{-1} \equiv \prod_{s \in S} sg(s \cdot g)^{-1} \bmod M$, and so the transfer map $v : G \to H/M$ is independent of the transversal used to calculate it.*

Proof. Let $t \in T$. There exists $s \in S$ such that $Ht = Hs$. This implies that there exists $h_t \in H$ such that $h_t t \in S$. This element is unique for if there exists $h' \in H$ such that $h't \in S$, then we have $Hh't = Ht = Hs$. We also have $Hh_t t = Ht$. Therefore, $Hh_t t = Hh't$. Since $h_t t, h't \in S$, we have $h_t t = h't$. Hence, $h_t = h'$. So for each $t \in T$, there is a unique element $h_t \in H$ such that $h_t t \in S$. Also, as t runs over T, the elements $h_t t$ run over S. Since $H(h_t t)g = H(t \cdot g)$, we can see that the unique element of S in this coset is $h_{t\cdot g}(t \cdot g)$. It follows that $(h_t t) \cdot g = h_{t\cdot g}(t \cdot g)$. Taking advantage of the fact that H/M is abelian, we see that $\prod_{s\in S} sg(s \cdot g)^{-1} \equiv \prod_{t\in T} h_t t g(h_{t\cdot g}(t \cdot g))^{-1} \equiv \prod_{t\in T} h_t t g(t \cdot g)^{-1} h_{t\cdot g}^{-1} \equiv \prod_{t\in T} tg(t \cdot g)^{-1} \prod_{t\in T} h_t \prod_{t\in T} h_{t\cdot g}^{-1} \bmod M$. Now, $t \cdot g$ runs over T as t does, so we have $(\prod_{t\in T} h_t)^{-1} \equiv \prod_{t\in T} h_{t\cdot g}^{-1} \bmod M$. Hence, $\prod_{t\in T} tg(t \cdot g)^{-1} \equiv \prod_{s\in S} sg(s \cdot g)^{-1} \bmod M$. The proof is now complete. □

The following is necessary if we are going to make much use of the transfer map.

Theorem 2.4. *The transfer map $v : G \to H/M$ is a homomorphism.*

Proof. Let $x, y \in G$. We need to show that $\pi(xy) \equiv \pi(x)\pi(y) \bmod M$. Taking advantage of the fact that H/M is abelian and since $t \cdot x$ runs over T as t does, we have $\pi(y) = \prod_{t\in T} ty(t \cdot y)^{-1} \equiv \prod_{t\in T} (t \cdot x)y((t \cdot x) \cdot y)^{-1} \equiv \prod_{t\in T} (t \cdot x)y(t \cdot xy)^{-1} \bmod M$. Hence, $\pi(x)\pi(y) \equiv \prod_{t\in T} tx(t\cdot x)^{-1} \prod_{t\in T} (t\cdot x)y(t\cdot xy)^{-1} \equiv \prod_{t\in T} tx(t\cdot x)^{-1}(t\cdot x)y(t\cdot xy)^{-1} = \prod_{t\in T} txy(t \cdot xy)^{-1} \bmod M$. Therefore, $\pi(xy) \equiv \pi(x)\pi(y) \bmod M$. The proof is now complete. □

Example 2.5. Let $G = \langle g \rangle$ be a cyclic group of order n. Suppose k is a divisor

of n. Let $H = \langle g^k \rangle$, and let $M = 1$. The set $T = \{1, g, g^2, \ldots, g^{k-1}\}$ gives a right transversal for $\langle g^k \rangle$ in $\langle g \rangle$. For $i \neq k-1$, we see that g^{i+1} is the element of T lying in the coset $\langle g^k \rangle g^i g$. That is, $g^i \cdot g = g^{i+1}$. If $i = k-1$, we have $g^i \cdot g = 1$. Thus, $v(g) = \pi(g) = \prod_{t \in T} tg(t \cdot g)^{-1} = (\prod_{i=0}^{k-2} g^i g(g^i \cdot g)^{-1})(g^{k-1} g(g^{k-1} \cdot g)^{-1}) = (\prod_{i=0}^{k-2} g^{i+1}(g^{i+1})^{-1})(g^{k-1} g(g^{k-1} \cdot g)^{-1}) = (g^{k-1} g(g^{k-1} \cdot g)^{-1}) = g^{k-1} g = g^k$. Therefore, $v(g) = g^k$. For any $x \in G = \langle g \rangle$, $x = g^j$ for some $j \in \{0, 1, \ldots, n-1\}$. Since v is a homomorphism, $v(x) = v(g^j) = (v(g))^j = g^{kj} = x^k$. Thus, for all $x \in G$, $v(x) = x^k$.

Example 2.6. Let p be an odd prime and let $G = \mathbb{Z}_p^\times$ be generated by g. (Note that G is cyclic of order $p-1$.) Let $H = \{1, -1\}$ and let $M = 1$. Set $p^* = (p-1)/2$.

(a) Since G is cyclic of order $p-1$ where p is odd, G contains only 1 element of order 2. That is, -1 is the only element of G of order 2. We have $(g^{p^*})^2 = g^{p-1} = 1$. Therefore, $g^{p^*} = -1$. So $H = \langle g^{p^*} \rangle$. By example 2.5, $v(g^j) = g^{jp^*} = (-1)^j$. For $a \in G$, $a = g^j$ for some j. We see that a is a square (modulo p) if and only if j is even. And j is even if and only if $v(a) = 1$. Thus $v(a) = (\frac{a}{p})$, the Legendre symbol.

(b) It is not hard to see that $T = \{1, 2, \ldots, p^*\}$ gives a transversal for $H = \{1, -1\}$ in $G = \mathbb{Z}_p^\times$ (where $p^* = (p-1)/2$). We will now compute the transfer v using this transversal. Let $LPR(x)$ denote the least positive residue of x modulo p. For $a \in G$ and $t \in T$, we see that $t \cdot a = LPR(ta)$ if $LPR(ta) < p^*$. Also, $t \cdot a \equiv -ta \pmod{p}$ if $LPR(ta) \geq p^*$. So for all $t \in T$ such that $LPR(ta) < p^*$, we have $ta(t \cdot a)^{-1} = 1$. So let $m(a)$ denote the number of $t \in T$ such that $LPR(ta) \geq p^*$. Then we see that $v(a) = (-1)^{m(a)}$. So combining the result of part (a) and the fact that the transfer is independent of the transversal used to calculate it, we have $(\frac{a}{p}) = (-1)^{m(a)}$. This

is known as Gauss's Lemma and is the key step in proving the Law of Quadratic Reciprocity. For $a = -1$ and $m(a) = p^*$ we have $(\frac{-1}{p}) = (-1)^{(p-1)/2}$.

The transfer map is not always surjective as we have seen in Example 2.2 (part a). The following lemma and corollaries provide conditions under which the transfer is surjective. This will give us some information on the kernel of the transfer homomorphism.

Lemma 2.7. *Let $G = HK$ be abelian with $H \cap K = 1$. Let $M = 1$. For $g = hk$, the transfer is given by $v(g) = h^{|K|}$.*

Proof. Let K be the transversal for H in G. Let $g = hk$. For $t \in K$ we have $t \cdot g = tk$ since $Htg = Hhtk = Htk$. Therefore, $v(g) = \prod_{k \in K} tg(t \cdot g)^{-1} = \prod_{k \in K} thk(tk)^{-1} = h^{|K|}$. □

Corollary 2.8. *Let $G = HK$ be abelian with $H \cap K = 1$. Let $M = 1$. If $|H|$ and $|K|$ are relatively prime, then the transfer $v : G \to H$ is surjective.*

Proof. Since $(|H|, |K|) = 1$, there are integers s and t with $s|H| + t|K| = 1$. Let $h \in H$. Then by Lemma 2.7, $v(h^t) = h^{t|K|} = h^{1-s|H|} = h$ since $h^{|H|} = 1$. Thus, v is surjective. □

Corollary 2.9. *Let G be abelian and P a Sylow p-subgroup. Then the transfer $v : G \to P$ is surjective*

Proof. G is abelian so we can write G as a direct sum of cyclic groups of order q^i for various primes q. P is the sum of those with $q = p$. Let M be the sum of those

with $q \neq p$. Then $G = PM$ and $P \cap M = 1$. Thus, it follows from Corollary 2.8 that v is surjective. $\square$

Computation of the transfer $v(g)$ turns out to be particularly easy if $g \in Z(G)$. The following application exploits this fact.

Theorem 2.10. *Let G be finite and suppose a Sylow p-subgroup of G is abelian. Then p does not divide $|Z(G) \cap G'|$.*

Proof. Let $P \in \mathrm{Syl}_p(G)$ and let T be a right transversal for P in G. Let $M = 1$ (trivial subgroup), and consider the transfer homomorphism $v : G \to P$. Suppose $z \in Z(G) \cap P \cap \ker(v)$. Let $t \in T$. Then $Ptz = Pzt = Pt$. So we have $t \cdot z = t$. Hence, $tz(t \cdot z)^{-1} = z$. Therefore, $v(z) = \prod_{t \in T} tz(t \cdot z)^{-1} = \prod_{t \in T} z = z^{|G:P|} = 1$. This implies that $|z|$ divides $|G : P|$. But $z \in P$, so $|z|$ is a power of p. Further, p does not divide $|G : P|$. So we must have $z = 1$. Therefore, $Z(G) \cap P \cap \ker(v) = 1$. Now, $v(G)$ is abelian, and $G/\ker(v) \cong v(G)$. The group G/G' is the largest abelian quotient of G. So it follows that $G' \subseteq \ker(v)$. Therefore, $P \cap Z(G) \cap G' = 1$. Since $Z(G) \cap G'$ is normal in G, $P(Z(G) \cap G') < G$. We have $|P(Z(G) \cap G')| = \frac{|P||Z(G) \cap G'|}{|P \cap Z(G) \cap G'|} = |P||Z(G) \cap G'|$. P is a Sylow p-subgroup of G, so it follows that p does not divide $|Z(G) \cap G'|$. The proof is now complete. $\square$

Corollary 2.11. *Let G have a cyclic Sylow p-subgroup. If $G \cong \Gamma/M$, where Γ is finite and $M \subseteq Z(\Gamma) \cap \Gamma'$, then p does not divide $|M|$.*

Proof. Let $P \in \mathrm{Syl}_p(\Gamma)$. Now, $M \lhd \Gamma$, so $P/(P \cap M) \cong PM/M$. It follows that PM/M is a p-subgroup of Γ/M. We have $|\Gamma/M : PM/M| = \frac{|\Gamma|}{|PM|}$. Also, $P < PM$,

so it follows that p does not divide $|\Gamma/M : PM/M| = \frac{|\Gamma|}{|PM|}$. Therefore, PM/M is a Sylow p-subgroup of Γ/M. Sylow p-subgroups are isomorphic, so every Sylow p-subgroup of Γ/M is cyclic (since G has a cyclic Sylow p-subgroup). Therefore, PM/M is cyclic. Hence, $P/(P\cap M)$ is cyclic. Now, $M \subseteq Z(\Gamma)\cap\Gamma'$, so it follows that $P\cap M \subseteq Z(P)$. Now, $P\cap M \trianglelefteq P$, and $Z(P) \trianglelefteq P$. So it follows that $P/Z(P) \cong (P/P\cap M)/(Z(P)/P\cap M)$. Further, $P/P\cap M$ is cyclic, so $(P/P\cap M)/(Z(P)/P\cap M)$ is cyclic. Hence, $P/Z(P)$ is cyclic. Therefore, P is abelian. By Theorem 2.10, it follows that p does not divide $|Z(\Gamma)\cap\Gamma'|$. Since $M < Z(\Gamma)\cap\Gamma'$, it now follows that p does not divide $|M|$. □

The following lemma is critical in the study of transfer theory.

Lemma 2.12. *(Transfer Evaluation)*

Let $M \lhd H \subseteq G$ with $|G : H| < \infty$ and H/M abelian, and let T be a right transversal for H in G. Then for each $g \in G$, there exists a subset $T_0 \subseteq T$ and positive integers n_t for $t \in T_0$ such that

1. $\sum n_t = |G : H|$,
2. $tg^{n_t}t^{-1} \in H$ *for all* $t \in T_0$, *and*
3. $\pi(g) \equiv \prod_{t\in T_0} tg^{n_t}t^{-1}$ *mod* M.

Also, if $|g| < \infty$, then

4. *each n_t divides $|g|$.*

Proof. G acts by right multiplication on the set of distinct right cosets of H in G. This action gives a corresponding right action of G on T. If $t \in T$, $g \in G$, then $t \cdot g$ is the unique element of T that lies in the right coset Htg. It follows that $\langle g \rangle$ acts on T under the same action and decomposes T into orbits. Letting T_0 be a set of representatives for these orbits and letting n_t denote the size of the orbit containing t, we see that $\sum_{t \in T_0} n_t = |T| = |G : H|$. So part 1 follows. Now consider $t \in T_0$. Let $[t]$ denote the orbit containing t (under the action of $\langle g \rangle$ on T), and let $\langle g \rangle_t$ denote the stabilizer of t. Then $n_t = |[t]| = |\langle g \rangle : \langle g \rangle_t|$. So we have $n_t |\langle g \rangle_t| = |g|$. So part 4 follows. Now, $\langle g \rangle$ is abelian, so $\langle g \rangle_t \trianglelefteq \langle g \rangle$. For $t \in T_0$ the map that sends $t \cdot g^i$ to $\langle g \rangle_t g^i$ is a bijection from $[t]$ onto $\langle g \rangle / \langle g \rangle_t$. The group $\langle g \rangle / \langle g \rangle_t$ is cyclic, and $|\langle g \rangle / \langle g \rangle_t| = |[t]| = n_t$. From the bijection given above and the fact that $\langle g \rangle / \langle g \rangle_t$ is a cyclic group generated by $\langle g \rangle_t g$ we can list the elements of $[t]$ explicitly as t, $t \cdot g$, $t \cdot g^2$, $\ldots t \cdot g^{n_t - 1}$. So we see that the permutation induced by g on the orbit containing t is an n_t-cycle. It follows that $t \cdot g^{n_t} = t$. We have $Ht = Htg^{n_t}$. This implies that $tg^{n_t}t^{-1} \in H$. Hence, part 2 now follows. Now, consider the elements of T in the orbit containing t. The contribution of these elements to the product $\pi(g) = \prod_{t \in T} tg(t \cdot g)^{-1}$ is $\prod_{i=0}^{n_t - 1} (t \cdot g^i) g (t \cdot g^{i+1})^{-1} = tg^{n_t}t^{-1}$. So it now follows that $\pi(g) \equiv \prod_{t \in T_0} tg^{n_t}t^{-1} \bmod M$. So part 3 follows, and the proof is now complete. $\square$

Example 2.13. Let $G = D_6$, $H = \langle f \rangle$, and $M = 1$. Let $T = \{1, r, \ldots, r^5\}$ be a transversal for H in G.

(a) $\langle f \rangle$ acts on T, decomposing T into orbits. Since $fr^i f = ffr^{-i} = r^{-i}$ for $0 \leq i \leq 5$, we see that $r^i \cdot f = r^{-i}$. So the action of $\langle f \rangle$ on T decomposes T into

the four orbits: $\{1\}, \{r, r^5\}, \{r^2, r^4\}$, and $\{r^3\}$. Let $T_0 = \{1, r, r^2, r^3\}$. Then $n_1 = 1$, $n_r = 2$, $n_{r^2} = 2$, and $n_{r^3} = 1$. By Lemma 2.12, we have $v(f) = \prod_{t \in T_0} tf^{n_t}t^{-1} = (f)(r^3 f r^{-3}) = f f r^{-3} r^{-3} = r^6 = 1$. So $v(f) = 1$.

(b) Now consider the action of $\langle r^3 \rangle$ on T. Here we see that $r^i \cdot r^3 = r^{3+i}$. So this action decomposes T into three orbits: $\{1, r^3\}$, $\{r, r^4\}$, $\{r^2, r^5\}$. Letting $T_0 = \{1, r, r^2\}$, we see that $n_1 = n_r = n_{r^2} = 2$. Since $(r^3)^{n_t} = 1$ for all $t \in T_0$, we see that $v(r^3) = \prod_{t \in T_0} t(r^3)^{n_t}t^{-1} = 1$. So $v(r^3) = 1$.

Corollary 2.14. *(Schur) Let $|G : Z(G)| = m < \infty$. Then the map $g \mapsto g^m$ is a homomorphism from G into $Z(G)$.*

Proof. We prove this corollary by showing that this map is the transfer map $v : G \to Z(G)$. Let $g \in G$. By the Transfer Evaluation Lemma we have that $v(g) = \pi(g) = \prod_{t \in T_0} tg^{n_t}t^{-1}$. We have $tg^{n_t}t^{-1} \in Z(G)$. So we have $tg^{n_t}t^{-1}t = t^2 g^{n_t}t^{-1}$. But $tg^{n_t} = t^2 g^{n_t}t^{-1}$ implies that $tg^{n_t}t^{-1} = g^{n_t}$. Therefore, $v(g) = \prod_{t \in T_0} g^{n_t} = g^{\Sigma n_t} = g^m$. The proof is now complete. □

One of our primary considerations will be the transfer of a group G into P/P', where P is a Sylow p-subgroup of G. The kernel of the transfer homomorphism $v : G \to P/P'$ will be useful in proving nonsimplicity theorems. If $v : G \to P/P'$ is surjective and P is a Sylow p-subgroup of G, then $v(P)$ is a Sylow p-subgroup of P/P'. Since P/P' is a p-group, $v(P) = v(G)$. Thus, $P \subset \ker(v)$ implies that $\ker(v) = G$. Therefore, $P \cap \ker(v)$ is proper in P if and only if $\ker(v)$ is proper in G. So if we want to know if $\ker(v)$ is proper in G, it suffices to compute $P \cap \ker(v)$.

We will see that this turns out to be the focal subgroup of P, which is given by the following definition.

Definition. Let $H \subseteq G$. Then the *focal subgroup* of H in G is $\mathrm{Foc}_G(H) = \langle x^{-1}y \mid x, y \in H \text{ and } x, y \text{ are } G-\text{conjugate}\rangle$.

Definition. We say that two conjugacy classes of H are *fused* in G if both are contained in the same G-conjugacy class. To say that there is *no fusion* in H means that if two elements of H are G-conjugate, then they are H-conjugate.

Let $x, h \in H$ and consider $[x, h] = x^{-1}x^h = x^{-1}h^{-1}xh \in H'$. Then x and $y = h^{-1}xh$ are clearly G-conjugate. So $x^{-1}y = x^{-1}h^{-1}xh = [x, h] \in \mathrm{Foc}_G(H)$. So we see that $H' \subseteq \mathrm{Foc}_G(H)$.

Lemma 2.15. *Let H be a subgroup of G. If there is no fusion in H, then $Foc_G(H) = H'$.*

Proof. If there is no fusion in H and if $x, y \in H$ and x, y are G-conjugate, then x, y are H-conjugate. So $y = h^{-1}xh$ for some $h \in H$. This implies that $x^{-1}y = x^{-1}h^{-1}xh = [x, h] \in H'$. Thus, $\mathrm{Foc}_G(H) \subseteq H'$. We have shown above that $H' \subseteq \mathrm{Foc}_G(H)$. This completes the proof. □

Example 2.16. Let $G = D_3$

(a) Let $H = \langle r\rangle$. Then H is abelian, so the H-conjugacy classes of H are $\{1\}$, $\{r\}$, and $\{r^2\}$. But r and r^2 are conjugate in G since $frf^{-1} = r^2$. Thus, the two classes $\{r\}$ and $\{r^2\}$ are fused in G since they are contained in the same G-

conjugacy class. Since r and r^2 are conjugate in G, $r^{-1}r^2 = r \in \mathrm{Foc}_G(H)$. Therefore, $\mathrm{Foc}_G(H) = H$.

(b) Let $H = \langle f \rangle$. Then H is abelian, so the H-conjugacy classes of H are $\{1\}$, and $\{f\}$. Now, 1 and f are not conjugate in G since $g(1)g^{-1} = 1$ for all $g \in G$. So in this case there is no fusion and we see that $\mathrm{Foc}_G(H) = 1$.

Theorem 2.17. *(Focal subgroup)*

Let G be finite. Suppose $H \subseteq G$ is a Hall subgroup and let $v : G \to H/H'$ be the transfer map. Then $Foc_G(H) = H \cap G' = H \cap ker(v)$.

Proof. Let $x, y \in H$ with $y = x^g$ for some $g \in G$. Then $x^{-1}g^{-1}xg = x^{-1}y = [x, g] \in G'$. Therefore $\mathrm{Foc}_G(H) \subseteq H \cap G'$. We also have that $G/\ker(v) \cong v(G) \subseteq H/H'$. Therefore, $G/\ker(v)$ is abelian. Hence, $G' \subseteq \ker(v)$. So we have $H \cap G' \subseteq H \cap \ker(v)$. So to complete the proof, we just need to show that $H \cap \ker(v) \subseteq \mathrm{Foc}_G(H)$. So assume $g \in H \cap \ker(v)$ and let $m = \sum n_t = |G : H|$. Using the Transfer Evaluation Lemma and the fact that H/H' is abelian, we have $\pi(g) \equiv \prod_{t \in T_0} tg^{n_t}t^{-1} \equiv g^m \prod_{t \in T_0} g^{-n_t}tg^{n_t}t^{-1} \bmod H'$. Now, each $g^{n_t} \in H$, and $tg^{n_t}t^{-1} \in H$ by the Transfer Evaluation Lemma. Therefore, each factor $g^{-n_t}tg^{n_t}t^{-1} \in Foc_G(H)$. And $g \in \ker(v)$, so $v(g) = H'\pi(g) = H'g^m \prod_{t \in T_0} g^{-n_t}tg^{n_t}t^{-1} = H'$. Now, let $h_1 \in H'$. Then $h_1 = h_2 g^m \prod_{t \in T_0} g^{-n_t}tg^{n_t}t^{-1}$ for some $h_2 \in H'$. So we have $g^m = h_2^{-1}h_1(\prod_{t \in T_0} g^{-n_t}tg^{n_t}t^{-1})^{-1}$. Since $H' \subseteq \mathrm{Foc}_G(H)$, it follows that $g^m \in \mathrm{Foc}_G(H)$. Since H is a Hall subgroup, its index is relatively prime to its order. As $g \in H$, it follows that $m = |G : H|$ is relatively prime to $|g|$. Now, $\langle g^m \rangle \leq \langle g \rangle$ and $|\langle g^m \rangle| = |g^m| = \frac{|g|}{(|g|,m)} = |g| = |\langle g \rangle|$. Hence, $\langle g \rangle = \langle g^m \rangle \subseteq \mathrm{Foc}_G(H)$. Therefore, $g \in \mathrm{Foc}_G(H)$. Hence, $H \cap \ker(v) \subseteq$

$\mathrm{Foc}_G(H)$. The proof is now complete. □

Corollary 2.18. *Let $P \in Syl_p(G)$ and suppose there is no fusion in P. then $G' \cap P = P'$.*

Proof. Since there is no fusion in P, Lemma 2.15 states that $\mathrm{Foc}_G(P) = P'$. □

Corollary 2.18 and the following lemma can be combined to provide more conditions under which the transfer $v : G \to P/P'$ is surjective.

Lemma 2.19. *Let $M \lhd H < G$ with H/M abelian. Let $v : G \to H/M$ be the transfer. Suppose A is a subgroup of G such that the following are true:*

1. *$A \lhd G$*
2. *$A \subseteq ker(v)$*
3. *$A \cap H = M$.*

We have maps

$$\bar{v} : G/A \to H/M$$

$$\varphi : H/M \to AH/A$$

$$\tilde{v} : G/A \to AH/A.$$

Here $\bar{v}$ is the map induced from v, φ is the usual isomorphism and $\tilde{v}$ is the transfer map from G/A into its subgroup AH/A. Then it follows that $(\varphi\bar{v})(Ag) = \tilde{v}(Ag)^{[A:M]}$.

Proof. The following will be used frequently throughout the proof:

For $h \in H$ and $a \in A$, there exist a', $a'' \in A$ such that $ah = ha'$ and $ha = a''h$.

This follows easily from the fact the A is normal in G.

Step 1. Let $S \subseteq G$ be such that $\{As : s \in S\}$ is a transversal for AH/A in G/A. Let $B \subseteq A$ be a transversal for M in A. Then BS is a transversal for H in G. To see this, let $g \in G$. There is an $s \in S$ such that $Ag \in (AH/A)As$. Therefore, $Ag = (Ah)(As) = Ahs$ for some $h \in H$. So for some $a \in A$,

$$g = ahs = ha's.$$

Thus, $g \in Ha's$. Now, $a' \in Mb$ for some $b \in B$ since B is a transversal for M in A. So $g \in HMbs = Hbs$. We have shown that $G \subseteq \bigcup_{\substack{b\in B \\ s\in S}} Hbs$. For uniqueness, suppose $Hb_1s_1 = Hb_2s_2$. Let $g \in Hb_1s_1$. Then for some $h \in H$, $g = hb_1s_1 = b_1''hs_1$. Then

$$Ag = Ahs_1 = (Ah)(As_1) \in (AH/A)(As_1)$$

Similarly, $Ag \in (AH/A)As_2$. Since $\{As : s \in S\}$ is a transversal for AH/A in G/A, we have $s_1 = s_2$. Thus, $Hb_1 = Hb_2$. Then $b_1b_2^{-1} \in H \cap A = M$, and $Mb_1 = Mb_2$. Since B is a transversal for M in A, $b_1 = b_2$. This completes the proof of Step 1.

Step 2. Suppose $s \cdot g = b_0s_0$. Then we have

1. For each $b \in B$ there exists $b_1 \in B$ such that $bs \cdot g = b_1s_0$.
2. $As \cdot Ag = As_0$

Since $Hsg = Hb_0s_0$, we have $sg = h_0b_0s_0$ for some $h_0 \in H$. Then

$$bsg = bh_0b_0s_0 = h_0b'b_0s_0.$$

Now $b'b_0 \in A = \cup Mb$, so there exist $b_1 \in B$, $m \in M$ such that $b'b_0 = mb_1$. So

$$Hbsg = Hh_0mb_1s_0 = Hb_1s_0$$

Therefore, $bs \cdot g = b_1s_0$. We have $sgs_0^{-1} = h_0b_0$. Let $h \in H$ and write $hh_0b_0 = ahh_0$ for some $a \in A$. Then $hh_0 = a^{-1}hh_0b_0 = a^{-1}hsgs_0^{-1}$. We have $hh_0s_0 = a^{-1}hsg$. So $Ahh_0s_0 = Ahsg$. Thus, $(Ahh_0)(As_0) = (Ah)(AsAg)$. Since h was arbitrary, $(AH/A)AsAg = (AH/A)As_0$. Therefore, $As \cdot Ag = As_0$.

Step 3. Now, $\bar{v}(Ag) = v(g)$ and $(\varphi\bar{v})(Ag) = Av(g)$. Further, $AM = A$ since $A \cap H = M$ implies that $M \subseteq A$. So we have

$$(\varphi\bar{v})(Ag) = A\prod_{\substack{s\in S\\ b\in B}} (bsg)(bs \cdot g)^{-1}$$

Fix $s \in S$. Since BS is a transversal for H in G, we may write $s \cdot g = b_0s_0$. By Step 2 we can write $bs \cdot g = \alpha(b)s_0$, where $\alpha(b) \in B$. As in the proof of Step 2, write $sg = h_0b_0s_0$ for some $h_0 \in H$. Then

$$\prod_{b\in B} (bsg)(bs \cdot g)^{-1} = \prod_{b\in B} bsgs_0^{-1}\alpha(b)^{-1}$$

$$= \prod_{b\in B} bh_0b_0\alpha(b)^{-1}.$$

Now we can change the order of multiplication keeping the same h_0 (but changing elements in $A \supseteq B$). So this product looks like $a^*h_0^{|B|}$, for some $a^* \in A$. The same trick shows that

$$(h_0b_0)^{|B|} = h_0b_0h_0b_0 \cdots = a^\dagger h_0^{|B|},$$

for some $a^\dagger \in A$. So we have

$$\prod_{b\in B}(bsg)(bs\cdot g)^{-1} = a^*(a^\dagger)^{-1}(h_0b_0)^{|B|} = a^*(a^\dagger)^{-1}(sgs_0^{-1})^{|B|}.$$

Thus,

$$(\varphi\bar{v})(Ag) = A\prod_{s\in S}(sgs_0^{-1})^{|B|},$$

where $s\cdot g = b_0s_0$.

Lastly, from Step 2 part 2,

$$\tilde{v}(Ag) = \prod_{s\in S}(AsAg)(As\cdot Ag)^{-1} = \prod_{s\in S}(AsAg)(As_0)^{-1}$$

$$= A\prod_{s\in S} sgs_0^{-1}.$$

It now follows that $(\varphi\bar{v})(Ag) = \tilde{v}(Ag)^{|B|}$. And $|B| = [A : M]$ since B is a transversal for M in A. The proof is now complete. □

Corollary 2.20. *Suppose P is a Sylow p-subgroup of G that has no fusion in G. Then the transfer $v : G \to P/P'$ is surjective.*

Proof. The conditions of the previous lemma are met with $A = G'$, $H = P$, $M = P'$. The fact that $G' \cap P = P'$ follows from Corollary 2.18. We continue with the same notation as the previous lemma and set $n = [G' : P']$. Now, let $\psi : PG'/G' \to PG'/G'$ be given by $\psi(x) = x^n$. Then ψ is a homomorphism since $PG'/G' \subseteq G/G'$ is abelian. The conclusion of the lemma can be written $\varphi\bar{v} = \psi\tilde{v}$. Now, $\tilde{v}$ is surjective by Corollary 2.9. Thus, $|G/G'| = |P/P'||\ker(\tilde{v})|$. Therefore, $\frac{|G'|}{|P'|} = \frac{|G|}{|\ker(\tilde{v})||P|}$. In particular, $n = [G' : P']$ is relatively prime to p. As $PG'/G' \cong P/P'$ is a p-group, it follows that ψ is injective and hence surjective. So $\psi\tilde{v} = \varphi\bar{v}$ is surjective, and as φ is bijective, $\bar{v}$ is surjective. Since $\bar{v}(G'x) = v(x)$, v is surjective. □

The following lemma will be helpful in computing the focal subgroup and proving a nice result which will be useful in proving claims involving nonsimplicity.

Lemma 2.21. *(Burnside) Let $P \in Syl_P(G)$ and suppose $x, y \in C_G(P)$ are conjugate in G. Then x and y are conjugate in $N_G(P)$.*

Proof. Let $y = x^g$ for some $g \in G$. Since $x, y \in C_G(P)$, we have $P \subseteq C_G(y)$ and $P \subseteq C_G(x)$. So we have $P^g \subseteq C_G(x)^g$. Now we prove that $C_G(x)^g = C_G(x^g)$. Let $y \in C_G(x)^g$. Then $y = g^{-1}g'g$ for some $g' \in C_G(x)$. Then $yg^{-1}xg = g^{-1}g'gg^{-1}xg = g^{-1}g'xg = g^{-1}xg'g = g^{-1}xgg^{-1}g'g = g^{-1}xgy$. Therefore, $y \in C_G(x^g)$. So $C_G(x)^g \subseteq C_G(x^g)$. Now suppose $g' \in C_G(x^g)$. Then $g'g^{-1}xg = g^{-1}xgg'$. Therefore, $g' = g^{-1}xgg'g^{-1}x^{-1}g$. Now, $g'g^{-1}xg = g^{-1}xgg'$ implies that $gg'g^{-1}xg = xgg'$. This implies that $x^2gg'g^{-1}x^{-1} = xgg'g^{-1}xgg^{-1}x^{-1} = xgg'g^{-1}$. Therefore, $xgg'g^{-1}x^{-1} \in C_G(x)$. Hence, $g' \in C_G(x)^g$. So $C_G(x^g) \subseteq C_G(x)^g$. It now follows that $P^g \subseteq C_G(x)^g = C_G(x^g) = C_G(y)$. So P and P^g are Sylow p-subgroups of $C_G(y)$. Since Sylow p-subgroups are conjugate, there exists $c \in C_G(y)$ such that $P^{gc} = P$. Therefore, $gc \in N_G(P)$ and we have $x^{gc} = y^c = y$. Hence, x and y are conjugate in $N_G(P)$. □

Definition. A subgroup N of a finite group G is said to be a *normal p-complement* in G (where p is a prime) if it is a normal subgroup having index a power of p and order not divisible by p.

Remark. We could also say a *normal p-complement* is a normal subgroup whose index is equal to the order of a Sylow p-subgroup of G.

The following can be a powerful tool in proving nonsimplicity since it gives a sufficient condition for a group to have a normal p-complement.

Theorem 2.22. *(Burnside) Let $P \in Syl_p(G)$ and suppose $P \subseteq Z(N_G(P))$. Then G has a normal p-complement.*

Proof. Let $x, y \in P$ be conjugate in G. Note that $P \subseteq Z(N_G(P))$ implies that P is abelian. So $x, y \in C_G(P)$, and therefore by Lemma 2.21, $y = x^n$ for some element $n \in N_G(P)$. But $P \subseteq Z(N_G(P))$, so we have $x^n = x$. Therefore, $x^{-1}y = 1$. It follows that $\mathrm{Foc}_G(P) = 1$. By our Focal Subgroup Theorem, $P \cap \ker(v) = 1$ where $v : G \to P$ is the transfer map. But $\ker(v)$ is normal in G, so $P\ker(v)$ is a subgroup of G of order $\frac{|P||\ker(v)|}{|P \cap \ker(v)|} = |P||\ker(v)|$. Since P is a Sylow p-subgroup of G, it follows that p does not divide $|\ker(v)|$. And $|G : \ker(v)| = |v(G)|$ is a p-power since $v(G)$ is a subgroup of P. Therefore, $\ker(v)$ is a normal p-complement for G. □

The following corollary is an application of Burnside's Theorem.

Corollary 2.23. *Suppose all Sylow subgroups of G are cyclic (for all primes). Then G is solvable.*

Proof. Let p be the smallest prime divisor of $|G|$, and let $P \in \mathrm{Syl}_p(G)$. Then P is normal in $N_G(P)$, so $N_G(P)$ acts by conjugation on P as automorphisms of P. This action induces a homomorphism $\sigma : N_G(P) \to \mathrm{Aut}(P)$ where $\ker(\sigma) = C_G(P)$. Therefore, $|N_G(P) : C_G(P)|$ divides $|\mathrm{Aut}(P)|$. But P is cyclic, so $\mathrm{Aut}(P) \cong (\mathbb{Z}/|P|\mathbb{Z})^\times$. Hence, $|\mathrm{Aut}(P)| = \phi(|P|)$, where ϕ is Euler's function. We can write $\phi(|P|) = (p-1)p^{a-1}$, where $p^a = |P|$. It follows that there is no prime larger

than p dividing $|N_G(P) : C_G(P)|$. And P is abelian, so $P \subseteq C_G(P)$. Therefore, $|N_G(P) : C_G(P)|$ is not divisible by p. By the choice of p, $|N_G(P) : C_G(P)|$ is not divisible by a prime smaller than p. Hence, $|N_G(P) : C_G(P)| = 1$. Now, $N_G(P) \subseteq C_G(P)$ implies that $P \subseteq Z(N_G(P))$. It now follows from Theorem 2.22 (Burnside) that G has a normal p-complement N. Further, N is a proper subgroup of G. So working by induction on $|G|$, we assume that N is solvable. And G/N is a p-group, so G/N is solvable. It now follows that G is solvable. □

Example 2.24. Burnside's Theorem can be used to show that certain numbers do not occur as orders of simple groups. For example, let $|G| = 12,100 = 2^2 \cdot 5^2 \cdot 11^2$. We have $n_{11} \equiv 1 \bmod 11$ and n_{11} divides $2^2 \cdot 5^2$. Hence, $n_{11} = 1$ and $n_{11} = 100$ are the only possibilities for the number of Sylow 11-subgroups of G. If $n_{11} = 1$, then of course the unique Sylow 11-subgroup of G is normal in G. Suppose $n_{11} = 100$. Let $P \in \mathrm{Syl}_{11}(G)$. Then $n_{11} = |G : N_G(P)| = 100$. This implies that $|N_G(P)| = |P|$. Therefore, $P = N_G(P)$ and P is abelian since its order is a square of a prime. Hence, $P = Z(P) = Z(N_G(P))$. By Burnside's Theorem, G has a normal 11-complement. So in neither case can G be simple.

Many other potential orders for simple groups can be eliminated by applying Burnside's Theorem. Among the integers between 1 and 200, 144 is a particulary nice example. We will encounter the case of 144 in Chapter 3.

Corollary 2.25. *Let $P \in Syl_p(G)$ and assume that P is abelian. Let $N = N_G(P)$. Then $G' \cap P = N' \cap P$.*

Proof. P is abelian, so $P \subseteq C_G(P)$. So it follows from Lemma 2.21 (Burnside) that if $x, y \in P$ are conjugate in G, then they are conjugate in N. So we have $\mathrm{Foc}_G(P) = \mathrm{Foc}_N(P)$. But P is a Hall subgroup of N and of G. So it now follows from the Focal subgroup theorem that $G' \cap P = N' \cap P$. □

We may consider whether or not Corollary 2.25 would remain true if we remove the condition that P is abelian. A MAPLE computation for the simple group of order 168, generated by (1,2,3,4,5,6,7) and (1,2,3)(4,5,7), gives a Sylow 2-subgroup P, where $N(P) = P$, and $N(P)' \cap P < G' \cap P$. Thus, the conclusion of Corollary 2.25 fails in this case.

In certain cases, Corollary 2.25 can help us establish the nonsimplicity of a group G by considering N in place of G. For instance, suppose P satisfies the hypotheses of Corollary 2.25, and N has a nontrivial p-group as a homomorphic image. Let $\varphi : N \to X$ be a surjective homomorphism where X is a nontrivial p-group. Suppose $P \subseteq N'$. Since P is a Sylow p-subgroup of N, it follows that $\varphi(P)$ is a Sylow p-subgroup of X. Now, X is a p-group, so $\varphi(P) = X$. Hence, X is abelian. So $P \subseteq N' \subseteq \ker(\varphi)$. It follows that p does not divide $\frac{|N|}{|\ker(\varphi)|}$. This is a contradiction since $N/\ker(\varphi) \cong X$, and X is p-power. Therefore P is not contained in N'. If $P \subseteq G'$, then by Corollary 2.25, $P = N' \cap P$. Hence, $P \subseteq N'$. This is a contradiction. Thus, P is not contained in G'. Therefore, $G' < G$. So if G is non-abelian, G cannot be simple.

Corollary 2.25 and Theorem 2.10 give us the following corollary.

Corollary 2.26. *Let $P \in Syl_p(G)$ be abelian and write $N = N_G(P)$. Then $Z(N) \cap P \cap G' = 1$*

Proof. P is an abelian Sylow p-subgroup of N. By Theorem 2.10, p does not divide $|Z(N) \cap N'|$. And $Z(N) \cap P \cap N' \subseteq P$ implies that $|Z(N) \cap P \cap N'|$ is a power of p. But $Z(N) \cap P \cap N' \subseteq Z(N) \cap N'$ implies that p does not divide $|Z(N) \cap P \cap N'|$. Therefore $Z(N) \cap P \cap N' = 1$. By Corollary 2.25, $P \cap N' = P \cap G'$. It now follows that $Z(N) \cap P \cap G' = 1$. □

The Feit-Thompson Theorem states that every group of odd order is solvable. So a finite non-abelian simple group has even order and therefore, has Sylow-2 subgroups. The classification of simple groups depends heavily on an exhaustive study of Sylow-2 subgroups. The following is a typical result and gives an application of Corollary 2.26.

Corollary 2.27. *Let G be a finite simple group having an abelian Sylow 2-subgroup of order 8. Then G contains no element of order 4.*

Proof. Let $P \in \mathrm{Syl}_2(G)$ and $N = N_G(P)$. Suppose to the contrary that G has an element g of order 4. It follows that $\langle g \rangle$ is a contained in a Sylow 2-subgroup of G. Sylow p-subgroups are isomorphic, so it follows that P contains an element of order 4. Any given abelian group of order 8 is isomorphic to one of the following: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Since $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ contains no element of order 4, P is isomorphic to either $\mathbb{Z}_8$, or $\mathbb{Z}_4 \times \mathbb{Z}_2$. In either case, P has a characteristic

subgroup Z of order 2. First suppose that $P \cong \mathbb{Z}_8$. Then P is cyclic, so P has a unique subgroup, Z of order 2. So it is clear that $\sigma(Z) = Z$ for any automorphism σ of P. Now suppose that $P \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. Then it follows that $Z = \{x^2 \mid x \in P\}$ is a characteristic subgroup of P of order 2. To see this let σ be an automorphism of P. Let $z \in Z$. Then $z = x^2$ for some $x \in P$. We have $\sigma(z) = \sigma(x^2) = (\sigma(x))^2 \in Z$. So $\sigma(Z) \subseteq Z$. And $\sigma(Z)$ cannot be trivial since σ is injective. So $\sigma(Z) = Z$. Therefore, Z is a characteristic subgroup of P of order 2. Since Z is a characteristic subgroup of P and $P \lhd N$, $Z \lhd N$. It follows that $Z \subseteq P \cap Z(N)$. To see this, let $z \in Z$. Clearly, $1 \in P \cap Z(N)$. So assume $z \neq 1$. We know $z \in P$. So we need to show that $z \in Z(N)$. So let $n \in N$. Since $Z \lhd N$, it follows that $nZn^{-1} = Z$. Therefore, $nzn^{-1} \in Z$. But $z \neq 1$, so $nzn^{-1} \neq 1$. Hence, $nzn^{-1} = z$ since $|Z| = 2$. It now follows that $z \in Z(N)$, and so $Z \subseteq P \cap Z(N)$. By Corollary 2.26, $Z(N) \cap P \cap G' = 1$. It follows that $Z \cap G' = 1$. Therefore, G' is a proper subgroup of G. And G' is non-trivial and normal in G. This is a contradiction since G is simple. $\square$

The following theorem from Frobenius gives several necessary and sufficient conditions for a finite group to have a normal p-complement. Unlike some of our previous results, the following statements do not require an abelian Sylow p-subgroup.

Theorem 2.28. *(Frobenius)*

Let $P \in Syl_p(G)$. Then the following are equivalent:

1. *G has a normal p-complement.*

2. *$N_G(U)$ has a normal p-complement for all p-subgroups $U \subseteq G$ with $U > 1$.*

3. *$N_G(U)/C_G(U)$ is a p-group for all p-subgroups $U \subseteq G$.*

4. *There is no fusion in P.*

We should comment here that the restriction $U > 1$ in statement (2) is not essential, however, (2) implies (1) would be redundant without it. If $U > 1$ is a p-subgroup, a subgroup of the form $N_G(U)$ is said to be *p-local* in G. We could say that (2) $\implies$ (1) says that the existence of a normal p-complement in G is determined "locally". Condition (3) says that whenever an element of G whose order is not divisible by p is in the normalizer of a p-subgroup of G, it is also in the centralizer. These elements are called the *p-regular* elements and do not act nontrivially on p-subgroups in G. We should also remark that the implication (3) $\implies$ (2) is not necessarily true unless (3) is assumed for all p-subgroups U. The implications (1) $\implies$ (2) and (2) $\implies$ (3) are not too difficult to prove. The most difficult implications to prove in Frobenius's Theorem are (3) $\implies$ (4) and (4) $\implies$ (1).

The following lemma is key to the proof that (3) implies (4) in Frobenius's Theorem.

Lemma 2.29. *Let G be finite and assume $N_G(U)/C_G(U)$ is a p-group for each p-subgroup $U \subseteq G$. Let $S, T \in Syl_p(G)$ and write $D = S \cap T$. Then $T = S^c$ for some element $c \in C_G(D)$.*

Proof. Suppose the result is false. Choose two Sylow p-subgroups S and T of G with $D = S \cap T$ as large as possible such that for all $c \in C_G(D), T \neq S^c$. Note that $S \neq T$. Let $N = N_G(D)$. Then $N \cap S \subseteq S$, so $N \cap S$ is a p-subgroup of N. Therefore, $N \cap S \subseteq S_0$ for some $S_0 \in \mathrm{Syl}_p(N)$. Similarly, $N \cap T \subseteq T_0$ for some $T_0 \in \mathrm{Syl}_p(N)$. And S_0 is a p-subgroup of G, so $S_0 \subseteq S_1$ for some $S_1 \in \mathrm{Syl}_p(G)$. Sylow p-subgroups are conjugate, so $T_0 = S_0^n$ for some $n \in N$. Let $T_1 = S_1^n$. So $T_1 \in \mathrm{Syl}_p(G)$ and $T_0 \subseteq T_1$. Since $S \neq T$, it follows that D is a proper subgroup of S. We have $S \cap S_1 \supseteq S \cap S_0 \supseteq S \cap N = N_S(D) > D$. (The fact that $N_S(D) > D$ follows from Theorem 1.3.) In a similar fashion $T_1 \cap T > D$. By our choice of S and T, it follows that $S_1 = S^a$ for some $a \in C_G(S \cap S_1) \subseteq C_G(D)$. Also, $T = T_1^b$ for some $b \in C_G(T_1 \cap T) \subseteq C_G(D)$. Now, $S_0 C_G(D)$ is a subgroup of N since $C_G(D)$ is normal in N. Let $|N| = p^\alpha m$ where p does not divide m. By our hypotheses, $N/C_G(D)$ is a p-group. This implies that $|C_G(D)| = p^\beta m$ where $\beta \leq \alpha$. In addition, $S_0 \cap C_G(D)$ is a p-subgroup of $C_G(D)$ since $S_0 \in \mathrm{Syl}_p(N)$. So $|S_0 \cap C_G(D)| = p^\gamma$ where $\gamma \leq \beta$. Hence, $|S_0 C_G(D)| = \frac{|S_0||C_G(D)|}{|S_0 \cap C_G(D)|} = \frac{p^\alpha p^\beta m}{p^\gamma} \geq |N|$. It now follows that $N = S_0 C_G(D)$. Therefore, $n = sc$ where $s \in S_0 \subseteq S_1$ and $c \in C_G(D)$. So $T_1 = S_1^{sc} = S_1^c$. It follows that $S^{acb} = S_1^{cb} = T_1^b = T$, and $acb \in C_G(D)$. We now have a contradiction to our choice of S and T. The proof is now complete. □

The following corollary gives the implication (3) $\implies$ (4) in Frobenius's The-

orem.

Corollary 2.30. *Let $P \in Syl_p(G)$ and assume that $N_G(U)/C_G(U)$ is a p-group for all p-subgroups $U \subseteq G$. Then there is no fusion in P.*

Proof. Let $x, y \in P$ with $y = x^g$ for some $g \in G$. We have $y = x^g \in P^g$. So $y \in P \cap P^g$. Since $P, P^g \in \mathrm{Syl}_p(G)$, by Lemma 2.29 we have $P^{gc} = P$ for some element $c \in C_G(P \cap P^g) \subseteq C_G(y)$. Now, $P \trianglelefteq N_G(P)$ and $C_G(P) \trianglelefteq N_G(P)$. So $PC_G(P)$ is a subgroup of $N_G(P)$, with $|PC_G(P)| = \frac{|P||C_G(P)|}{|P \cap C_G(P)|}$. But $P \cap C_G(P) \subseteq P$ and $P \cap C_G(P) \subseteq C_G(P)$ implies that $P \cap C_G(P)$ has p-power order and $|P \cap C_G(P)|$ divides $|C_G(P)|$. Now, $N_G(P)/C_G(P)$ is a p-group and $P \in \mathrm{Syl}_p(N_G(P))$ implies that $\frac{|P||C_G(P)|}{|P \cap C_G(P)|} \geq |N_G(P)|$. It follows that $N_G(P) = PC_G(P)$. Also, $gc \in N_G(P)$ since $P^{gc} = P$. So we may write $gc = ua$ where $u \in P$ and $a \in C_G(P)$. Now $x^u \in P$, so $a \in C_G(x^u)$. We have $x^u = x^{ua} = x^{gc} = y^c = y$. And $u \in P$, so we have shown that x and y are P-conjugate. Hence, there is no fusion in P. □

The following theorem gives the implication (4) $\implies$ (1) in Frobenius's Theorem.

Theorem 2.31. *Let $P \in Syl_p(G)$ and assume that there is no fusion in P. Then G has a normal p-complement.*

Proof. Let $K \lhd G$ be minimal such that G/K is a p-group. (It may occur that $K = G$.) We just need to show that p does not divide $|K|$. Suppose that p divides $|K : K'|$. Assume that $|K : K'| = p^\alpha m$ where p does not divide m. The group K/K' is abelian, so we can write it as a direct product of cyclic subgroups of prime-

power order. Let H_1 be the product of the p-power factors and H_2 the product of the factors whose orders divide m. Then $K/K' \cong H_1 \times H_2$ where $|H_1| = p^\alpha$ and $|H_2| = m$. If $(x, y) \in H_1 \times H_2$, $(x \in H_1, y \in H_2)$ then $|(x, y)| = \text{lcm}(|x|, |y|)$. So we see that $H_2 = \{z \in K/K' \mid z^m = 1\}$. Now if σ is an automorphism of $H_1 \times H_2$, then $z^m = 1$ implies that $\sigma(z)^m = 1$. So σ maps H_2 into H_2. Hence, K/K' has a proper characteristic subgroup of p-power index. Denote this subgroup by H/K'. $K \lhd G$ implies that $K/K' \lhd G/K'$. We have H/K' is a characteristic subgroup of K/K'. Also, $K/K' \lhd G/K'$. Therefore, $H/K' \lhd G/K'$. Hence, $H \lhd G$. So H is a normal subgroup of G smaller than K having p-power index in G. This is a contradition to the definition of K. So it follows that p does not divide $|K : K'|$. Now, let $Q = P \cap K$. Since $K \lhd G$, it follows that PK is a subgroup of G with $|PK| = \frac{|P||K|}{|P \cap K|}$. If $Q \notin \text{Syl}_p(K)$, then p would divide $\frac{|K|}{|P \cap K|}$ contradicting the fact that $|PK|$ divides $|G|$ since $P \in \text{Syl}_p(G)$. Therefore, $Q \in \text{Syl}_p(K)$. Suppose Q is not contained in K'. Let $q \in Q$, $q \notin K'$. Consider the element $qK' \in K/K'$. Clearly, $|qK'|$ divides $|q|$. Also, q has p-power order, and $q \notin K'$. So $|qK'| = p^b$, for some $b \geq 1$. But $|qK'|$ divides $|K/K'|$ which contradicts the fact that p does not divide $|K/K'|$. Hence, $Q \subseteq K'$. By the Focal Subgroup Theorem, $Q \cap K' = \text{Foc}_K(Q)$. We have $Q = Q \cap K'$ since $Q \subseteq K'$. Hence, $Q = \text{Foc}_K(Q)$. On the other hand, suppose $x, y \in Q$ are K-conjugate. Then x and y are elements of P that are G-conjugate. Since there is no fusion in P, $y = x^u$ for some $u \in P$. Therefore, $x^{-1}y = [x, u] \in [Q, P]$. So $Q = \text{Foc}_K(Q) \subseteq [Q, P]$. It follows that $Q \subseteq [Q, P, P, \ldots, P] \subseteq P^n$ for all positive integers n. But P is nilpotent, so by Theorem 1.5 it follows that some term P^n of

its lower central series is trivial. This forces $Q = 1$. Hence, p does not divide $|K|$. The proof is now complete. □

Proof of Frobenius Theorem:

Proof. Suppose (1) is true and let N be a normal p-complement in G. Let $H \subseteq G$ be any subgroup. We will show that H has a normal p-complement, and this will prove (2). It is easy to verify that $H \cap N \trianglelefteq H$, and $|H \cap N|$ is not divisible by p. Since $H/H \cap N \cong HN/N$, we have that $|H : H \cap N| = |HN : N|$. Also, $|HN : N|$ divides $|G : N|$, which is a p-power. Hence, $H \cap N$ is a normal p-complement in H. This proves (2). Now assume (2) and let $U \subseteq G$ be a p-subgroup. If $U = 1$, then $N_G(U)/C_G(U)$ is a p-group. So we may assume $U > 1$. Let M be a normal p-complement for $N_G(U)$. Since p does not divide the order of any element of M and U is a p-subgroup, $M \cap U = 1$. Now suppose $m \in M$ and let $u \in U$. Since both M and U are normal in $N_G(U)$, $uMu^{-1} = M$ and $mUm^{-1} = U$. So $umu^{-1} = m'$ and $mum^{-1} = u'$ for some $m' \in M$ and $u' \in U$. Now $mum^{-1}u^{-1} = u'u^{-1} \in U$ and $umu^{-1}m^{-1} = m'm^{-1} \in M$. We have $(m'm^{-1})^{-1} = mum^{-1}u^{-1} \in M$. So $mum^{-1}u^{-1} \in M \cap U = 1$ implies that $mu = um$. Hence, $m \in C_G(U)$. We have shown that $M \subseteq C_G(U)$. Thus $|N_G(U) : C_G(U)|$ divides $|N_G(U) : M|$, and is therefore, p-power. This proves (3). The fact that (3) implies (4) was Corollary 2.30. (4) implies (1) was given by Theorem 2.31. The proof of Frobenius's Theorem is now complete. □

The following corollary is a nice application of Frobenius's Theorem.

Corollary 2.32. *Let $|G| = p^a m$, were p is prime and p does not divide m. Suppose that $(m, p^e - 1) = 1$ for all integers e with $1 \leq e \leq a$. Then G has a normal p-complement.*

Proof. Suppose to the contrary that G does not have a normal p-complement. By Frobenius's Theorem, there exists a p-subgroup $U \subseteq G$ such that $N_G(U)/C_G(U)$ is not a p-group. Now, $N_G(U)/C_G(U)$ is isomorphic to a subgroup of $\mathrm{Aut}(U)$. It follows that $\mathrm{Aut}(U)$ contains an element σ of prime order q where q divides m. Let $V = \{u \in U \mid u\sigma = u\}$. It is easy to see that V is a subgroup of U. Since σ is not the identity V is a proper subgroup of U. For $\phi \in \mathrm{Aut}(U)$ and $u \in U$, $\phi \cdot u = \phi(u)$ gives an action of $\mathrm{Aut}(U)$ on U. This gives an action of $\langle\sigma\rangle$ on U. Let $\langle\sigma\rangle_x$ denote the stabilizer of $x \in U - V$ under the action of $\langle\sigma\rangle$ on U. Note that $\langle\sigma\rangle_x$ is a subgroup of $\langle\sigma\rangle$. Since $|\langle\sigma\rangle_x|$ divides q and $x \notin V$, $\langle\sigma\rangle_x = 1$. It follows that all the elements of $U - V$ lie in orbits of size q under $\langle\sigma\rangle$. Hence, q divides $|U| - |V| = |V|(|U : V| - 1)$. Since q does not divide $|V|$, q divides $|U : V| - 1$. Now, $|U : V| = p^e$ for some exponent e with $1 \leq e \leq a$. This is a contraction. Therefore, G has a normal p-complement. □

Corollary 2.33. *If $|G| = 2k$ for some odd integer k greater than 1, then G is not simple.*

Proof. Suppose $|G| = 2k$ for some odd integer k greater than 1. Then 2 does not divide k and $(k, 1) = 1$. By Corollary 2.32, it follows that G has a normal subgroup of order k. Thus, G is not simple. □

Corollary 2.34. *If G is simple with $|G| = 8m$, then one of 2,3, or 7 must divide m.*

Proof. Suppose G is simple with $|G| = 8m$ and none of 2,3, or 7 divide m. (Note that m must be greater than 1) Then $|G| = 2^3 m$ where 2 does not divide m. We have $(m, 1) = (m, 3) = (m, 7) = 1$. By Corollary 2.32, it follows that G has a normal subgroup of order m. This contradicts the simplicity of G. Hence, one of 2,3, or 7 must divide m if G is a simple group of order $8m$. □

CHAPTER 3

COMPUTATIONS

Before we begin a lengthy analysis that will involve disproving existence of simple groups for orders from 1-200 (in which they do not occur), we should give some basic results that follow from Sylow's Theorems. These results will make the task more convenient and immediately eliminate potential orders.

Proposition 3.1. *If $|G| = pq$ for primes p and q with $p < q$, then G is not simple*

Proof. By Sylow's Theorems, $n_q \equiv 1 \bmod q$ and n_q divides p. It clearly follows that $n_q = 1$. Therefore, a Sylow q-subgroup of G is normal. □

The two propositions that follow are from [3].

Proposition 3.2. *If G is a finite group and H is a proper subgroup of G such that $|G|$ does not divide $|G : H|!$, then H contains a nontrivial normal subgroup of G. In particular, G is not simple.*

Proof. G acts by left multiplication on the set X of left cosets of H in G, inducing a permutation representation of G into the symmetric group on X. This permutation representation $\alpha : G \to S_X$ is defined by $\alpha(g) = \sigma_g$ where $\sigma_g : X \to X$ is defined for $xH \in X$ by $\sigma_g(xH) = gxH$. If $g \in \ker(\alpha)$, then $\sigma_g(xH) = xH$ for all $xH \in X$. In particular, $\sigma_g(H) = gH = H$. Hence, $g \in H$. So $\ker(\alpha) \subseteq H$. Therefore, $\ker(\alpha)$ is a normal subgroup of G contained in H. And $G/\ker(\alpha)$ is isomorphic to a subgroup of S_X which has order $|G : H|!$. Hence, $\frac{|G|}{|\ker(\alpha)|}$ divides $|G : H|!$. Since $|G|$ does not divide $|G : H|!$, $\ker(\alpha)$ is nontrivial. It now follows that G is not simple. □

Proposition 3.3. *If a finite non-abelian simple group G has a subgroup of index n, then G is isomorphic to a subgroup of A_n.*

Proof. Let H be a subgroup of index n in G. Consider the non-trivial homomorphism from G into S_n from the proof of Proposition 3.2. Since G is simple and the kernel of a homomorphism is a normal subgroup, we have an injective homomorphism from G into S_n. Therefore, G is isomorphic to a subgroup of S_n. Any subgroup of S_n consists of all even permutations, or half of the elements are even permutations and half of the elements are odd permutations. If G were isomorphic to a subgroup of S_n of the latter type, then the even permutations of this subgroup would form a subgroup of index 2. Subgroups of index 2 are normal. Therefore, G would have a proper, non-trivial normal subgroup. Hence, G is isomorphic to a subgroup of S_n consisting entirely of even permutations. It now follows that G is isomorphic to a subgroup of A_n. □

Proposition 3.4. *If P and P' are Sylow p-subgroups of order p, then $P \cap P' = 1$*

Proposition 3.5. *p-groups have non-trivial centers.*

The integers 2 and 3 are primes, so of course 2 and 3 occur as orders of simple groups. Neither $\mathbb{Z}_4$ nor $\mathbb{Z}_2 \times \mathbb{Z}_2$ is simple, so 4 is not the order of a simple group.

[Skipping n=5, 6, 7, 8, 9, 10 ,11 brings us to:]

$n = 12$: By Sylow's Theorems, a group of order 12 has a subgroup of index 3. 12 does not divide 3!. So by Proposition 3.2, 12 does not occur as the order of a simple

group.

[Skipping n=13, 14, 15, 16, 17 brings us to :]

$n = 18$: $n_3 \equiv 1 \pmod 3$ and divides 2. Thus, $n_3 = 1$ and G is not simple.

$n = 20$: $n_5 \equiv 1 \pmod 5$ and divides 4. Therefore, n_5=1 and G is not simple.

[Skipping n=21, 22, 23 brings us to:]

$n = 24$: Any group of order $24=2^3 \cdot 3$ has a subgroup of index 3, and 24 does not divide 3!. It follows from Proposition 3.2 that 24 is not the order of a simple group.

[Skipping n=25, 26, 27 brings us to:]

n=28: $n_7 \equiv 1 \pmod 7$ and divides 4. Thus, n_7=1 and G is not simple.

[Skipping n=29 brings us to:]

n=30: If n_3=1 or n_5=1, then G is simple. Suppose not. Then $n_3 = 10$ and $n_5 = 6$. This gives $10 \cdot 2 = 20$ elements of order 3 and $6 \cdot 4 = 24$ elements of order 5. But G has only 30 elements. This is a contradiction. Thus, n_3=1 or n_5=1. So G is not simple.

[Skipping n=31, 32, 33, 34, 35 brings us to:]

$n = 36 = 2^2 \cdot 3^2$: Any group of order $36=2^2 \cdot 3^2$ has a subgroup of index 4, and 36

does not divide 4!=24. Hence, 36 does not occur as the order of a simple group.

[Skipping n=37, 38, 39 brings us to:]

$n = 40 = 2^3 \cdot 5$: $n_5 \equiv 1 \pmod 5$ and divides 8. Hence, $n_5 = 1$ and G is not simple.

$n = 42 = 2 \cdot 3 \cdot 7$: $n_7 \equiv 1 \pmod 7$ and divides 6. So $n_7 = 1$ and G is not simple.

n=44=$2^2 \cdot 11$: $n_{11} \equiv 1 \pmod{11}$ and divides 4. Thus, $n_{11} = 1$ and G is not simple.

n=45=$3^2 \cdot 5$: $n_5 \equiv 1 \pmod 5$ and divides 9. So $n_5 = 1$ and G is not simple.

[Skipping n=46, 47 brings us to:]

$n = 48$: Any group of order 48=$2^4 \cdot 3$ has a subgroup of index 3. Since 48 does not divide 3!, It follows from Proposition 3.2 that 48 does not occur as the order of a simple group.

[Skipping n=49 brings us to:]

$n = 50 = 2 \cdot 5^2$: $n_5 \equiv 1 \pmod 5$ and divides 2. Hence, $n_5 = 1$ and G is not simple.

[Skipping $n = 51$ brings us to:]

$n = 52 = 2^2 \cdot 13$: Clearly a Sylow 13-subgroup is normal. So G is not simple.

$n = 54 = 2 \cdot 3^3$: A Sylow 3-subgroup is normal, so G is not simple.

[Skipping n=55 brings us to:]

$n = 56$: There are a couple approaches we may take in dealing with 56. We may make a counting argument or we may apply Burnside's Theorem. First we make a counting argument. So assume G is a simple group of order $56=2^3 \cdot 7$. Then we must have $n_7 = 8$ and $n_2 = 7$. The 8 Sylow 7-subgroups account for 48 elements of order 7. Just 1 Sylow 2-subgroup will give 8 new elements, which gives us all the elements of G. But there are 7 Sylow 2-subgroups. This is a contradiction. Therefore, 56 is not the order of a simple group. Now consider another approach. Suppose G is a simple group of order $56=2^3 \cdot 7$. Let $P \in \mathrm{Syl}_7(G)$. We must have $n_7 = 8$. It follows that $|N_G(P)| = 7$. Therefore $P = N_G(P)$. And P is abelian, so $P = Z(P)$. Hence, $P = Z(P) = Z(N_G(P))$. It follows from Burnside's Theorem that G has a normal subgroup of order 8, contradicting the simplicity of G.

[Skipping n=57, 58, 59, 60 (A_5 is simple), 61, 62 brings us to:]

$n = 63 = 3^2 \cdot 7$: $n_7 \equiv 1 \pmod 7$ and divides 9. Therefore, $n_7 = 1$ and G is not simple.

[Skipping n=64, 65 brings us to:]

$n = 66 = 2 \cdot 3 \cdot 11$: $n_{11} \equiv 1 \pmod{11}$ and divides 6. So $n_{11} = 1$ and G is not simple.

$n = 68 = 2^2 \cdot 17$: Clearly a Sylow 17-subgroup is normal. So G is not simple.

[Skipping n=69 brings us to:]

$n = 70 = 2 \cdot 5 \cdot 7$: $n_7 \equiv 1 \pmod{7}$ and divides 10. Thus, $n_7 = 1$ and G is not simple.

[Skipping n=71 brings us to:]

$n = 72 = 2^3 \cdot 3^2$: $n_3 \equiv 1 \bmod 3$ and n_3 divides 8. So if $|G| = 72$, $n_3 = 1$ or $n_3 = 4$. If $n_3 = 1$, the Sylow 3-subgroup of G is normal. Suppose $n_3 = 4$. Let P be a Sylow 3-subgroup of G. Then $N_G(P)$ is a proper subgroup of G, and $|G|$ does not divide $n_3! = 4! = |G : N_G(P)|!$. By Proposition 3.2, $N_G(P)$ contains a nontrivial normal subgroup of G. It now follows that G is not simple. So no group of order 72 is simple.

[Skipping n=73, 74 brings us to:]

$n = 75 = 3 \cdot 5^2$: $n_5 \equiv 1 \pmod{5}$ and divides 3. Therefore, $n_5 = 1$ and G is not simple.

$n = 76 = 2^2 \cdot 19$: Clearly a Sylow 19-subgroup is normal. So G is not simple.

[Skipping n=77 brings us to:]

$n = 78 = 2 \cdot 3 \cdot 13$: $n_{13} \equiv 1 \pmod{13}$ and divides 6. So $n_{13} = 1$ and G is not simple.

$n = 80$: Suppose $|G| = 80 = 2^4 \cdot 5$. By Sylow's Theorem, G has a subgroup of order 16. Since 80 does not divide 5!, Proposition 3.2 states that G is not simple. So no group of order 80 is simple.

[Skipping n=81, 82, 83 brings us to:]

$n = 84 = 2^2 \cdot 3 \cdot 7$: $n_7 \equiv 1 \pmod{7}$ and divides 12. Thus, $n_7 = 1$ and G is not simple.

[Skipping n=85, 86, 87 brings us to:]

$n = 88 = 2^3 \cdot 11$: Clearly a Sylow 11-subgroup is normal. So G is not simple.

$n = 90 = 2 \cdot 3^2 \cdot 5$: Here n_3=1 or 10 and n_5=1 or 6. We cannot count elements since the Sylow 3-subgroups have order 9. Assume $n_3 = 10$ and $n_5 = 6$. Then a Sylow 3-subgroup has index 10 in G, and a Sylow 5-subgroup has index 18 in G. The normalizer of a Sylow 3-subgroup has index 10 in G, and the normalizer of a Sylow 5-subgroup has index 6 in G. Now, $| G |= 90$ divides 6!, 10!, and 18!. So we cannot use Proposition 3.2 here. So transfer theory is necessary here. Indeed, G is not simple by Corollary 2.33.

[Skipping n=91 brings us to:]

$n = 92 = 2^2 \cdot 23$: Clearly a Sylow 23-subgroup of G is normal. So G is not simple.

[Skipping n=93, 94, 95 brings us to:]

$n = 96 = 2^5 \cdot 3$: Any group of order 96 has a subgroup of order 32. This subgroup has index 3 in G. Since 96 does not divide 3!, G is not simple by Proposition 3.2. Therefore, no group of order 96 is simple.

$n = 98 = 2 \cdot 7^2$: A Sylow 7-subgroup of G is normal. Hence, 98 does not occur as the order of a simple group.

$n = 99 = 3^2 \cdot 11$: A Sylow 11-subgroup is normal. So G is not simple.

$n = 100 = 2^2 \cdot 5^2$: $n_5 \equiv 1 \pmod 5$ and divides 4. Thus, $n_5 = 1$ and G is not simple.

$n = 102 = 2 \cdot 3 \cdot 17$: $n_{17} \equiv 1 \pmod{17}$ and divides 6. Therefore, $n_{17} = 1$ and G is not simple.

$n = 104 = 2^3 \cdot 13$: $n_{13} \equiv 1 \pmod{13}$ and divides 8. Thus, $n_{13} = 1$ and G is not simple.

$n = 105 = 3 \cdot 5 \cdot 7$: We can prove that no group of order 105 is simple in a

couple ways. Suppose $|G| = 105$ Then $n_3 = 1$ or 7, $n_5 = 1$ or 21, $n_7 = 1$ or 15. If G is simple, then G has 7 Sylow 3-subgroups, 21 Sylow 5-subgroups, and 15 Sylow 7-subgroups. Any two Sylow 3-subgroups must intersect in the identity. The same holds true for the Sylow 5-subgroups and the Sylow 7-subgroups. So the 7 Sylow 3-subgroups account for 14 non-identity elements of G. The 21 Sylow 5-subgroups give 84 new non-identity elements. The 15 Sylow 7-subgroups account for 90 more elements of G. This contradicts the fact that G has only 105 elements. Therefore, G must contain either a normal Sylow 3-subgroup, a normal Sylow 5-subgroup, or a normal Sylow 7-subgroup. Hence, no group of order 105 is simple.

Alternatively, we could just apply Corollary 2.32 with p=3 to see that no group of order 105 is simple. With p=3, Corollary 2.32 states that a group of order 105 has a normal subgroup of order 35.

[Skipping n=106, 107 brings us to:]

$n = 108 = 2^2 \cdot 3^3$: By Sylow's Theorems, G has a subgroup of index 4. Because 108 does not divide 4!, it follows from Proposition 3.2 that G is not simple. Hence, 108 does not occur as the order of a simple group.

$n = 110 = 2 \cdot 5 \cdot 11$: $n_{11} \equiv 1 \pmod{11}$ and divides 10. So $n_{11} = 1$ and G is not simple.

[Skipping n=111 brings us to:]

$n = 112 = 2^4 \cdot 7$: Suppose G were a simple group of order 112. Necessarily then G is non-abelian. By Sylow's Theorems, G has a subgroup of index 7. By Proposition 3.3, G is isomorphic to a subgroup of A_7. But $|G|$=112 does not divide $|A_7|$=2520. This is a contradiction. Therefore, 112 does not occur as the order of a simple group.

$n = 114 = 2 \cdot 3 \cdot 19$: $n_{19} \equiv 1 \pmod{19}$ and divides 6. Thus, $n_{19} = 1$ and G is not simple.

[Skipping n=115 brings us to:]

$n = 116 = 2^2 \cdot 29$: Clearly a Sylow 29-subgroup is normal. So G is not simple.

$n = 117 = 3^2 \cdot 13$: $n_{13} \equiv 1 \pmod{13}$ and divides 9. So $n_{13} = 1$ and G is not simple.

[Skipping n=118, 119 brings us to:]

$n = 120 = 2^3 \cdot 3 \cdot 5$: This is a somewhat difficult case. Suppose G is a simple group of order 120. Then we must have $n_5 = 6$. Let $P \in \mathrm{Syl}_5(G)$. It follows that $|G : N_G(P)| = 6$. The group G acts by left multiplication on the 6 left cosets of $N_G(P)$ in G. This action induces a homomorphism $\varphi : G \to S_6$ with $\ker(\varphi) \subseteq N_G(P)$. The kernel of a homomorphism is a normal subgroup, so $\ker(\varphi)$ is trivial. Hence $G \cong \varphi(G) \subseteq S_6$. Let $\varphi(G) = H$. $A_6 \lhd S_6$ and $H \subseteq S_6$, so it follows that HA_6 is a subgroup of S_6 having order $\frac{|H||A_6|}{|H \cap A_6|} = \frac{|H||S_6|}{2 \cdot |H \cap A_6|}$. It follows that $H \cap A_6$

has index 1 or 2 in H. The group H is simple, so $H \cap A_6$ cannot have index 2 in H. Hence, $H \cap A_6 = H$. So it follows that $H \subseteq A_6$. Now, $|A_6 : H| = \frac{360}{120} = 3$. Since $|A_6|$ does not divide $|A_6 : H|!$, it follows from Proposition 3.2 that A_6 is not simple. This is a contradiction since A_n is simple for all $n \geq 5$. It now follows that no group of order 120 is simple.

[Skipping n=121, 122, 123 brings us to:]

$n = 124 = 2^2 \cdot 31$: A Sylow 31-subgroup is normal. So G is not simple.

[Skipping n=125 brings us to:]

$n = 126 = 2 \cdot 3^2 \cdot 7$: Then $n_7 \equiv 1 \bmod 7$ and n_7 divides 18. Hence, the only possibility for n_7 is 1. So the Sylow-7 subgroup of G is normal. Therefore, no group of order 126 is simple.

[Skipping n=127, 128, 129 brings us to:]

$n = 130 = 2 \cdot 5 \cdot 13$: $n_{13} \equiv 1 \pmod{13}$ and divides 10. So $n_{13} = 1$ and G is not simple.

$n = 132 = 2^2 \cdot 3 \cdot 11$: Suppose G is a simple group of order 132. Then we must have $n_{11} = 12$. If n_3 were 4, Proposition 3.2 would give a contradiction. It follows that $n_3 = 22$. $n_{11} = 12$ and $n_3 = 22$ gives 164 non-identity elements of G, thereby contradicting the order of G. It now follows that no group of order 132 is simple.

[Skipping n=133, 134 brings us to:] $n = 135 = 3^3 \cdot 5$: $n_5 \equiv 1 \pmod 5$ and divides 27. The only possibility for n_5 is 1. So a Sylow 5-subgroup of G is normal. Hence, G is not simple.

$n = 136 = 2^3 \cdot 17$: Here we see that a Sylow 17-subgroup is normal. So G is not simple.

$n = 138 = 2 \cdot 3 \cdot 23$: $n_{23} \equiv 1 \pmod{23}$ and divides 6. So $n_{23} = 1$ and G is not simple.

$n = 140 = 2^2 \cdot 5 \cdot 7$: $n_7 \equiv 1 \pmod 7$ and divides 20. The only possibility for n_7 is 1. So the Sylow 7-subgroup of G is normal. Therefore, 140 is not the order of a simple group.

[Skipping n=141, 142, 143 brings us to:]

$n = 144$: The case of 144 provides a nice illustration of how useful transfer theory can be. First we prove that 144 is not the order of a simple group using only Sylow's Theorems and counting arguments. The proof is adapted from [3]. So assume G is a simple group of order $144 = 2^4 \cdot 3^2$. Then $n_3 = 4$ or 16 and $n_2 \geq 3$. n_3 cannot be 4 by Proposition 3.2. So $n_3 = 16$. Suppose every pair of Sylow 3-subgroups of G had only the identity in common. Then the Sylow 3-subgroups would give 128 non-

identity elements. The Sylow 2-subgroups of G would produce more than 16 new elements of G, contradicting the order of G. Hence, there exists $H_1, H_2 \in \mathrm{Syl}_3(G)$, with $|H_1 \cap H_2| = 3$. H_1 and H_2 have order 9, so both are abelian. Therefore, $H_1 \cap H_2$ is normal in both H_1 and H_2. So $N_G(H_1 \cap H_2)$ contains both H_1 and H_2. Consider the set H_1H_2. We see that H_1H_2 is contained in $N_G(H_1 \cap H_2)$. Therefore, $|N_G(H_1 \cap H_2)| \geq |H_1H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|} = 27$. Let $k = |N_G(H_1 \cap H_2)|$. So we know that $k \geq 27$ and k is a multiple of 9 dividing 144. Hence, $k \geq 36$ which implies that $|G : N_G(H_1 \cap H_2)| \leq 4$. Proposition 3.2 now gives a contradiction. It now follows that 144 does not occur as the order of a simple group.

Burnside's Theorem provides a much simpler argument. If $|G| = 144 = 2^4 \cdot 3^2$, Let $P \in \mathrm{Syl}_3(G)$. Since P has order 9, P is abelian. Therefore, $P = Z(P)$. Since $n_3 = 16$, $|N_G(P)| = 9$. Hence, $P = N_G(P)$. So $Z(N_G(P)) = Z(P) = P$. By Burnside's Theorem, G has a normal subgroup of order 16. Hence, G is not simple.

[Skipping n=145, 146 brings us to:]

$n = 147 = 3 \cdot 7^2$: $n_7 \equiv 1 \pmod 7$ and divides 3. So $n_7 = 1$ and G is not simple.

$n = 148 = 2^2 \cdot 37$: $n_{37} \equiv 1 \pmod{37}$ and divides 4. Thus, $n_{37} = 1$ and G is not simple.

$n = 150 = 2 \cdot 3 \cdot 5^2$: Let $|G| = 150$. Then G has a subgroup of index 6, and 150 does not divide 6!=720. By Proposition 3.2, G is not simple. The simplicity of

G is also given by Corollary 2.33. Hence, no group of order 150 is simple.

$n = 152 = 2^3 \cdot 19$: $n_{19} \equiv 1 \pmod{19}$ and divides 8. Hence, $n_{19} = 1$ and G is not simple.

$n = 153 = 3^2 \cdot 17$: $n_{17} \equiv 1 \pmod{17}$ and divides 9. Therefore, $n_{17} = 1$ and G is not simple.

$n = 154 = 2 \cdot 7 \cdot 11$: $n_{11} \equiv 1 \pmod{11}$ and divides 14. So $n_{11} = 1$ and G is not simple.

[Skipping n=155 brings us to:]

$n = 156 = 2^2 \cdot 3 \cdot 13$: $n_{13} \equiv 1 \pmod{13}$ and divides 12. So $n_{13} = 1$ and G is not simple.

[Skipping n=157, 158, 159 brings us to:]

$n = 160 = 2^5 \cdot 5$: Let $|G| = 160$. Then G has a subgroup of index 5 and 160 does not divide 5!=120. By Proposition 3.2, G is not simple. So 160 is not the order of a simple group.

[Skipping n=161 brings us to:]

$n = 162 = 2 \cdot 3^4$: $n_3 \equiv 1 \pmod{3}$ and divides 2. So $n_3 = 1$ and G is not simple.

$n = 164 = 2^2 \cdot 41$: $n_{41} \equiv 1 \pmod{41}$ and divides 4. Thus, $n_{41} = 1$ and G is not simple.

$n = 165 = 3 \cdot 5 \cdot 11$: $n_{11} \equiv 1 \pmod{11}$ and divides 15. So $n_{11} = 1$ and G is not simple.

[Skipping n=166, 167, 168, (it is known that there is a simple group of order 168), 169 brings us to:]

$n = 170 = 2 \cdot 5 \cdot 17$: $n_{17} \equiv 1 \pmod{17}$ and divides 10. So $n_{17} = 1$ and G is not simple.

$n = 171 = 3^2 \cdot 19$: $n_{19} \equiv 1 \pmod{19}$ and divides 9. Thus, $n_{19} = 1$ and G is not simple.

$n = 172 = 2^2 \cdot 43$: It is easy to see that a Sylow 43-subgroup is normal. So G is not simple.

$n = 174 = 2 \cdot 3 \cdot 29$: $n_{29} \equiv 1 \pmod{29}$ and divides 6. So $n_{29} = 1$ and G is not simple.

$n = 175 = 5^2 \cdot 7$: If $|G| = 175$ it is easy to see that the only possibility for n_7

is 1. So the Sylow 7-subgroup of G is normal. Therefore, 175 does not occur as the order of a simple group.

$n = 176 = 2^4 \cdot 11$: $n_{11} \equiv 1 \pmod{11}$ and divides 16. So $n_{11} = 1$ and G is not simple.

[Skipping n=177, 178, 179 brings us to:]

$n = 180$: This is another case that can be simplified with the use of Burnside's Theorem. Suppose G is a simple group of order $180=2^2 \cdot 3^2 \cdot 5$. Then we have $n_5 = 6$ or 36 and $n_3 = 10$. (n_3 cannot be 4 by Proposition 3.2) First suppose $n_5 = 36$. This will give 144 elements of order 5. If each pair of the Sylow 3-subgroups intersects in just the identity, we will have 80 new non-identity elements in G. This contradicts the order of G. So there are Sylow 3-subgroups H_1 and H_2 in G where $|H_1 \cap H_2| = 3$. By the same argument used for the case of 144, we have $|N_G(H_1 \cap H_2)| \geq |H_1 H_2| = \frac{9 \cdot 9}{3} = 27$. Since $|N_G(H_1 \cap H_2)|$ divides 180, $|N_G(H_1 \cap H_2)| = 9 \cdot k$ where $k \geq 3$ and k divides 20. It follows that $|N_G(H_1 \cap H_2)| \geq 36$. So $|G : N_G(H_1 \cap H_2)| \leq 5$. Proposition 3.2 now gives a contradiction. Therefore, we can assume that $n_5 = 6$. Since $n_5 = 6$, we know that the normalizer of a Sylow 5-subgroup of G has index 6. By Proposition 3.3, G is isomorphic to a subgroup of A_6. We also know that the order of the normalizer of a Sylow 5-subgroup of G has order 30. Since every group of order 30 has an element of order 15, G contains an element of order 15. (Every group of order 30

has a subgroup of order 15) But A_6 has no element of order 15. We have arrived at a contradiction. It now follows that 180 is not the order of a simple group. The preceding proof was adapted from [3].

We now show that a contradiction to the claim that $n_5 = 36$ can be arrived at much quicker with the use of Burnside's Theorem. Suppose $|G| = 180 = 2^2 \cdot 3^2 \cdot 5$ where G is simple. Suppose $n_5 = 36$ and let P be a Sylow 5-subgroup of G. Then P is cyclic, and hence, abelian. So $P = Z(P)$. $n_5 = 36$ implies that $|N_G(P)| = 5$. Hence, $N_G(P) = P$. We have $P = Z(P) = Z(N_G(P))$. It now follows from Burnside's Theorem that G has normal subgroup of order 36, contradicting the simplicity of G.

$n = 182 = 2 \cdot 7 \cdot 13$: Let $|G| = 182$. Then it is easy to see that the only possibility for n_7 is 1. Therefore, the Sylow 7-subgroup of G is normal. Hence, no group of order 182 is simple.

[Skipping n=183 brings us to:]

$n = 184 = 2^3 \cdot 23$: $n_{23} \equiv 1 \pmod{23}$ and divides 8. Hence, $n_{23} = 1$ and G is not simple.

[Skipping n=185 brings us to:]

$n = 186 = 2 \cdot 3 \cdot 31$: $n_{31} \equiv 1 \pmod{31}$ and divides 6. Therefore, $n_{31} = 1$ and G is not simple.

[Skipping n=187 brings us to:]

$n = 188 = 2^2 \cdot 47$: $n_{47} \equiv 1 \pmod{47}$ and divides 4. So $n_{47} = 1$ and G is not simple.

$n = 189 = 3^3 \cdot 7$: $n_7 \equiv 1 \pmod{7}$ and divides 27. The only possibility for n_7 is 1. So a Sylow 7-subgroup of G is normal. Hence, G is not simple.

$n = 190 = 2 \cdot 5 \cdot 19$: $n_{19} \equiv 1 \pmod{19}$ and divides 10. Thus, $n_{19} = 1$ and G is not simple.

$n = 192 = 2^6 \cdot 3$: By Sylow's Theorems, G has a subgroup of index 3. 192 does not divide 3!. By Proposition 3.2, G is not simple.

[Skipping n=193, 194 brings us to:]

$n = 195 = 3 \cdot 5 \cdot 13$: $n_{13} \equiv 1 \pmod{13}$ and divides 15. Thus, $n_{13} = 1$ and G is not simple.

$n = 196 = 2^2 \cdot 7^2$: $n_7 \equiv 1 \pmod{7}$ and divides 4. Hence, $n_7 = 1$ and G is not simple.

$n = 198 = 2 \cdot 3^2 \cdot 11$: $n_{11} \equiv 1 \pmod{11}$ and divides 18. So $n_{11} = 1$ and G is not simple.

$n = 200 = 2^3 \cdot 5^2$: $n_5 \equiv 1 \pmod 5$ and divides 8. Therefore, $n_5 = 1$ and G is not simple.

The fact that none of the integers from 201 through 239 occur as orders of non-abelian simple groups is not difficult to prove. 240 provides an interesting case. Suppose G is a simple group of order $240=2^4 \cdot 3 \cdot 5$. It follows that $n_5 = 6$ or 16. If $n_5 = 6$, then G has a subgroup of index 6. By Proposition 3.3, G is isomorphic to a subgroup of A_6. But $240 = |G|$ does not divide $360=|A_6|$. This is a contradiction. Therefore, $n_5 = 16$. Now, let $P \in \mathrm{Syl}_5(G)$. We have $|N_G(P)| = 15$. This implies that $N_G(P)$ is cyclic, and we have $Z(N_G(P)) = N_G(P)$. Hence, $P \subseteq Z(N_G(P))$. By Burnside's Theorem, G has a normal subgroup of order 48. This is a contradiction. Therefore, 240 is not the order of a simple group. Transfer theory can be applied to the case of $252=2^2 \cdot 3^2 \cdot 7$. Suppose G is a simple group of order 252. Then it follows that $n_7 = 36$. If P is a Sylow p-subgroup of G, then $|N_G(P)| = 7$. Therefore, $P = N_G(P)$. Since P is abelian, $P = Z(P) = Z(N_G(P))$. By Burnside's Theorem, G has a normal subgroup of order 36. This is a contradiction. Hence, 252 does not occur as the order of a simple group.

The following propositon will be helpful in proving a claim that will help us disprove existence of non-abelian simple groups for particular orders. Most of the following material has been adapted from [2].

Proposition 3.6. *(Frattini) Let G be a finite group, let H be a normal subgroup of G and let P be a Sylow p-subgroup of H. Then $G = HN_G(P)$ and $|G : H|$ divides*

$|NG(P)|$.

Proof. $H \trianglelefteq G$, so $HN_G(P)$ is a subgroup of G. Let $g \in G$. We have $P^g \subseteq H^g = H$. Since $P, P^g \in \mathrm{Syl}_p(H)$, there exists $x \in H$ such that $P^g = P^x$. Therefore, $gx^{-1} \in N_G(P)$. It follows that $g \in N_G(P)x$, and so $g \in N_G(P)H = HN_G(P)$. (Recall that $H \trianglelefteq G$.) We have shown that $G \subseteq N_G(P)H$. Thus, $G = N_G(P)H = HN_G(P)$. It follows from the second isomorphism theorem that $|G : H| = |N_G(P) : N_G(P) \cap H|$. Hence, $|G : H|$ divides $|N_G(P)|$. □

Suppose G is a simple group of order n with a proper subgroup of index k. Then we have shown above that G is isomorphic to a subgroup of S_k. Before we present the next two propostions we should comment that if this is the case, then we identify G with its isomorphic copy contained in S_k and simply view G as a subgroup of S_k.

Proposition 3.7. *If G has no subgroup of index 2 and $G \subseteq S_k$, then $G \subseteq A_k$.*

Proof. Suppose to the contrary that G is not contained in A_k. Then A_k is a proper subgroup of GA_k, and $|GA_k| = \frac{|G||A_k|}{|G \cap A_k|} = \frac{|G||S_k|}{2|G \cap A_k|}$. G is not contained in A_k, so half the elements of G are even permutations and half the elements of G are odd. It follows that $|G \cap A_k| = \frac{1}{2}|G|$. This implies that $\frac{|G||S_k|}{2|G \cap A_k|} = |Sk|$. Hence, $GA_k = S_k$. By the second isomorphism theorem, $2{=}|S_k : A_k| = |GA_k : A_k| = |G : G \cap A_k|$. So $G \cap A_k$ is a subgroup of index 2 in G. This is a contradiction. It follows that $G \subseteq A_k$. □

Proposition 3.8. *If $P \in Syl_p(S_k)$ for some odd prime p, then $P \in Syl_p(A_k)$ and*

$|N_{A_k}(P)| = \frac{1}{2}|N_{S_k}(P)|$.

Proof. Suppose $P \in \mathrm{Syl}_p(S_k)$ for some odd prime p. By Propositon 3.7, $P \subseteq A_k$. Hence, $P \in \mathrm{Syl}_p(A_k)$. By Proposition 3.6, $S_k = N_{S_k}(P)A_k$. So it follows that $N_{S_k}(P)$ is not contained in A_k. So half the elements of $N_{S_k}(P)$ are even permutations and half are odd permutations. Therefore, $N_{S_k}(P) \cap A_k = N_{A_k}(P)$ is a subgroup of index 2 in $N_{S_k}(P)$. It now follows that $|N_{A_k}(P)| = \frac{1}{2}|N_{S_k}(P)|$. □

The following observation may help us eliminate some potential orders of non-abelian simple groups.

Suppose G is a simple group of order n containing a proper subgroup of index k. Then as we have noted above, we may write $G \subseteq S_k$. Assume further that $k = p$ or $k = p + 1$ where p is a prime. It follows that p^2 does not divide $k!$, so Sylow p-subgroups of G are Sylow p-subgroups of S_k. It is clear that

the no. of Sylow p-subgroups of S_k=$\frac{\text{the no. of } p\text{-cycles}}{\text{the no. of } p\text{-cycles in a Sylow } p\text{-subgroup}}$

$=\frac{k(k-1)\cdots(k-p+1)}{p(p-1)}$. This gives the index in S_k of the normalizer of a Sylow p-subgroup of S_k. Hence, $|N_{S_k}(P)| = p(p-1)$ in the case of $k = p$ or $p+1$. We also have that $|N_G(P)|$ divides $p(p-1)$.

The above results may be applied to the case of $264=2^3 \cdot 3 \cdot 11$. Suppose G is a simple group of order 264. Then it follows that $n_{11} = 12$. By Proposition 3.7, $G \subseteq A_{12}$. If P is a Sylow 11-subgroup of G, then we see that $|N_G(P)| = 22$. By our above observation and Proposition 3.8, $|N_{A_{12}}(P)| = \frac{1}{2}|N_{S_{12}}(P)| = \frac{1}{2}11(11-1) = 55$. However, $N_G(P) \subseteq N_{A_{12}}(P)$, and 22 does not divide 55. This is a contradiction. It now follows that 264 does not occur as the order of a simple group.

The case of $396=2^2 \cdot 3^2 \cdot 11$ is an interesting example. Suppose G is a simple group of order 396. We have $n_{11} = 12$. If P is a Sylow 11-subgroup of G, then it follows that $|N_G(P)| = 33$. By our above observations, $G \subseteq S_{12}$, $P \in \mathrm{Syl}_{11}(S_{12})$, and $|N_{S_{12}}(P)| = 110$. However, $N_G(P) \subseteq N_{S_{12}}(P)$. This implies that 33 divides 110. This is a contradiction. It follows that 396 does not occur as the order of a simple group.

We now show that this proof can be simplified with the use of Burnside's Theorem. Suppose G is a simple group of order 396. If P is a Sylow 11-subgroup of G, then $|N_G(P)| = 33$. Every group of order 33 is cyclic. So it follows that $N_G(P)$ is abelian. So we have that $Z(N_G(P)) = N_G(P)$. Hence, $P \subseteq Z(N_G(P))$. By Burnside's Theorem it follows that G has a normal subgroup of order 36. This is a contradiction. Hence, no group of order 396 is simple.

REFERENCES

[1] Isaacs, M., *Algebra: A Graduate Course*, American Mathematical Society, Providence, 1994.

[2] Dummit, D.S. and Foote, R.M., *Abstract Algebra*, Third edition, John Wiley and Sons, Inc., 2004.

[3] Gallian, J.A., *Contemporary Abstract Algebra*, Sixth edition, Houghton Mifflin Company, Boston, 2006.

VITA

Graduate School
Southern Illinois University

Nicolas David Meyer Date of Birth: October 18, 1985

800 E. Grand Ave., Carbondale, Illinois 62901

707 Westchester Ln., Bolingbrook, Illinois 60440

ndmeyer1888@comcast.net

Benedictine University, Lisle, Illinois
Bachelor of Science, Mathematics, May 2009

Special Honors and Awards: Master's Fellowship for the 2009-2010 academic year at Southern Illinois University Carbondale

Research Paper Title:
Transfer Theory and its Applications to the Study of Simple Groups

Major Professor: Dr. R. Fitzgerald